

# TIBCO WebFOCUS®

## Security and Administration

*Release 9.1.0*  
*October 2022*  
*DN4501303.1022*





# Contents

---

<b>1. TIBCO WebFOCUS Components and Deployment Options .....</b>	<b>17</b>
The TIBCO WebFOCUS Security Model .....	17
TIBCO WebFOCUS Components .....	19
TIBCO WebFOCUS Deployment Options .....	20
Basic Internal Deployment Pattern.....	20
Basic External Deployment Pattern.....	21
Mixed Deployment Pattern.....	23
<b>2. Configuring the TIBCO WebFOCUS Reporting Server .....</b>	<b>25</b>
TIBCO WebFOCUS Reporting Server Security Modes .....	25
TIBCO WebFOCUS Reporting Server Browser Interface.....	27
Navigating to the Reporting Server Browser Interface.....	27
IP Restriction Filtering .....	29
Configuring a Security Provider on the TIBCO WebFOCUS Reporting Server .....	30
Configuring an LDAP or Active Directory Security Provider on the TIBCO WebFOCUS Reporting Server.....	31
Understanding LDAP Security Provider Properties.....	33
Configuring a Custom RDBMS Security Provider on the TIBCO WebFOCUS Reporting Server.....	38
Changing the Security Provider Configuration.....	41
Configuring Trusted Connections .....	49
Configuring TIBCO WebFOCUS for SSL .....	51
TIBCO WebFOCUS Reporting Server Profiles .....	56
Sending Variables to the TIBCO WebFOCUS Reporting Server Profile.....	57
<b>3. Configuring the TIBCO WebFOCUS Client .....</b>	<b>61</b>
TIBCO WebFOCUS Configuration Files .....	61
Using the TIBCO WebFOCUS Administration Console .....	62
Opening the TIBCO WebFOCUS Administration Console.....	62
Opening the ReportCaster Console.....	65
Working With Home Pages.....	65
Navigating the TIBCO WebFOCUS Administration Console.....	69
Navigating the Configuration Tab.....	70

Navigating the Security Tab. ....	74
Navigating the ReportCaster Tab. ....	75
Navigating the Diagnostics Tab. ....	75
Using the TIBCO WebFOCUS Administration Console Menu Bar. ....	76
Using the Licenses Menu. ....	76
Reviewing Client License Information. ....	77
Reviewing User Audit Information. ....	81
Understanding TIBCO WebFOCUS Product Editions. ....	84
Understanding TIBCO WebFOCUS Product Editions. ....	85
Understanding Legacy Product Editions. ....	85
Clearing the Cache. ....	87
Closing the TIBCO WebFOCUS Administration Console. ....	87
Opening TIBCO WebFOCUS Administration Console Help. ....	88
Configuring and Customizing Your Environment . ....	88
TIBCO WebFOCUS Reporting Server Settings. ....	88
Configuring TIBCO WebFOCUS Reporting Server Connections. ....	97
Reconnecting the Client to the Repository. ....	102
Alternate Server Mapping. ....	102
Managing Clustered Servers. ....	104
Managing Legacy Cluster Configurations. ....	106
Using Client Profiles. ....	106
The Client Site Profile. ....	106
The Universal Profile. ....	108
Managing Distribution Directories. ....	109
Granting Access to Distribution Directory Nodes. ....	114
Understanding Application Settings. ....	122
Managing Automatic Sign Outs. ....	123
Understanding Custom Settings. ....	124
Understanding NLS Settings. ....	125
Customizing the Dynamic Language Switch. ....	127
Understanding Redirection Settings. ....	129
Redirecting and Saving File Output. ....	130
Specifying an Output File Name Within a Report Request. ....	131



Adding a Date and Time to the PCHOLD AS Filename.....	132
Saving GRAPH (PNG, SVG, GIF, JPEG, or JPG) Requests.....	133
Understanding InfoAssist Properties.....	133
Understanding TIBCO WebFOCUS Designer Properties.....	133
Understanding the Role Update Utility.....	133
Working With HTML5 Chart Extensions.....	135
Understanding HTML5 Chart Extension Entries.....	136
Understanding the HTML5 Chart Extensions Enable/Enabled Check Box.....	136
Uploading Additional HTML5 Chart Extensions Using the Upload and Install Extensions Page.....	137
Configuring TIBCO WebFOCUS Security .....	142
Understanding Internal Security Page Settings.....	143
Understanding External Security Page Settings.....	147
Using Advanced Settings.....	149
Configuring Security Zones.....	152
Understanding the Default Zone Configuration.....	152
Understanding the Mobile Zone Configuration.....	153
Understanding the Portlet Zone Configuration.....	153
Understanding the Alternate Zone Configuration.....	153
Enabling Security Zones.....	154
Working With the Authentication Page.....	154
Managing the Allowed Host Names List.....	157
Configuring Cross-Origin Settings.....	159
Defining Origins.....	160
Allowing Embedding.....	161
Allowing Cross-Origin Resource Sharing.....	164
Configuring HTTP Strict Transport Security (HSTS) Within a Security Zone. . .	167
Understanding the HTTP Strict Transport Security Setting Dialog Box. .	168
Understanding the Request Matching Page.....	170
Understanding the URL Request Pattern Tab.....	170
Understanding the IP Address of the Client/Last Proxy Tab.....	170
Importing and Exporting Security Zone Settings.....	171
Working With TIBCO WebFOCUS Diagnostics .....	172

Reviewing Version Information. ....	173
Reviewing Client Verification . ....	174
Monitoring the HTTP Request Info Page. ....	175
Monitoring the JVM Property Information Page. ....	176
Monitoring the Memory Information (K) Tab. ....	177
Memory Usage Statistics Table. ....	178
Understanding Entry Highlights. ....	179
Memory Allocation Guidelines. ....	180
System Properties List. ....	180
Monitoring JVM Performance. ....	181
Monitoring Sessions. ....	183
Viewing Sessions. ....	186
Reviewing the Session Viewer Main Page. ....	187
Reviewing the Session Details Page. ....	191
Reviewing Trace Entries. ....	194
Reviewing Expanded URL Details. ....	195
Reviewing Reporting Server Request Details. ....	197
Reviewing Reporting Server Response Details. ....	198
Saving Trace Files. ....	199
Session Folder Contents. ....	200
Working With Log Files . ....	201
Working With Log Pages. ....	203
Working With Application Log Files. ....	204
Working With Application Log Pages . ....	205
Working With LRU Cache Statistics. ....	206
Understanding the Cache Statistics Page Layout. ....	207
Understanding Cache Entries. ....	207
Understanding Cache Statistics. ....	208
Understanding Cache Group Entries. ....	210
DBA Password Settings . ....	212
Obtaining the Identity of the User. ....	212
Deferred Receipt Processing. ....	213
Stopping a Report Request . ....	214

<b>4. Authentication and Authorization .....</b>	<b>217</b>
Understanding Authentication .....	218
Supporting Different Security Models in Different Environments.....	219
The Remember Me Feature.....	219
Configuring Pre-Authentication, External Authentication or External Authorization .....	221
Security Zones .....	224
Specifying a Sign-out URL by Zone.....	226
Anonymous Access .....	227
Making BI Portals Available to Anonymous Users.....	231
Distinguishing Basic Portals from Collaborative Portals and Designer Portals.....	232
Form Based Authentication.....	233
Internal Authentication .....	233
Pre-Authentication .....	234
Configuring Pre-Authentication With Central Authentication Service (CAS).....	234
Configuring Pre-Authentication with HTTP BASIC Authentication.....	237
Configuring Pre-Authentication With Java Container Security.....	238
Configuring Pre-Authentication With OpenID Connect.....	239
Configuring OpenID Connect Authentication Settings at an Identity Provider.....	240
Configuring OpenID Connect Authentication Settings Within TIBCO WebFOCUS....	241
Configuring OpenID Connect Pre-Authentication with Google.....	243
Configuring OpenID Connect Pre-Authentication with Keycloak.....	245
Configuring Pre-Authentication With Other OpenID Connect Identity Providers.....	247
Configuring Pre-Authentication With Web Access Management Systems.....	250
Configuring Pre-Authentication With Integrated Windows Authentication.....	253
Configuring Pre-Authentication With Custom Single Sign On (SSO) Solutions.....	255
Configuring Kerberos for Single Sign On.....	256
Limitations on Pre-authentication Using Kerberos.....	256
Understanding Constrained Delegation Versus Unconstrained Delegation.....	257
Pre-Installation Steps for Kerberos in Windows Active Directory.....	258
Examples of Check Service Principal Name (SPN) Results.....	261
Examples of a Successful Service Principal Name (SPN) Registration.....	262
Host Header Support for Kerberos.....	272

TIBCO WebFOCUS Reporting Server Configuration Requirements for Kerberos	
Constrained Delegation. ....	275
TIBCO WebFOCUS Client Configuration Steps for Kerberos. ....	276
Web Browser Configuration for Kerberos. ....	279
Configuring Google Chrome for Kerberos. ....	285
Configuring Support for ReportCaster for Kerberos. ....	294
Configuring Support for Large Tickets for Kerberos. ....	295
Setting Up TIBCO WebFOCUS With Kerberos in a Multi-Domain Environment. ....	295
Configuring Pre-Authentication with SAML ....	300
SAML Authentication Prerequisites. ....	302
Configuring Trusted Ticket Authentication for Embedded BI Applications. ....	310
Tracing the Trusted Ticket Authentication Workflow. ....	311
Using the Alternate Security Zone for Trusted Ticket Authentication. ....	314
Trusted Ticket Authentication Configuration Overview. ....	315
Evaluating Trusted Ticket Authentication. ....	316
External Authentication ....	321
Understanding Active Directory and LDAP Authentication. ....	322
Configuring Authentication by Information in an RDBMS Table. ....	324
Understanding Authorization ....	325
Understanding Internal Authorization ....	326
Understanding External Authorization ....	326
EXTERNAL and EXTERNALONLY Options. ....	327
AUTOADD. ....	328
Limitations When Configuring External Authentication With External Authorization. ....	328
Special Considerations When Using User Profile Attributes for Authorization. ....	329
Configuring External Authorization. ....	330
Group Mapping. ....	333
Special Considerations for Microsoft Office Drill-Down Links ....	336
Special Considerations for TIBCO WebFOCUS Deployments With Separate ReportCaster	
Installations ....	337
<b>5. TIBCO WebFOCUS Administration .....</b>	<b>339</b>
Assessing Security Requirements ....	339

IBFS Filesystem and Subsystems .....	340
Using Variables in IBFS Paths.....	345
Components of the Security System .....	347
Privileges.....	347
Types of Privileges.....	347
Local Privileges.....	348
Session Privileges.....	348
Hybrid Privileges.....	349
Resources.....	350
Viewing Resource Components .....	350
User and Group Resources.....	356
Explicit and Implicit Groups.....	357
Private and Published Resources.....	358
Private Resources.....	358
Published Resources.....	359
Shared Resources.....	359
Understanding How Sharing Affects Folders and Resources in the Hierarchy.....	361
Sharing Resources.....	362
Rules.....	362
Effective Policy.....	363
Order of Precedence.....	363
Policy Design .....	366
Group Design.....	366
Role Design.....	367
Rule Design.....	368
Working With Folders .....	369
Understanding Workspaces .....	375
Understanding My Workspace.....	376
Understanding the Getting Started Workspace.....	377
Understanding Resource Templates.....	378
Understanding Resource Template Groups.....	378
Naming a New Workspace.....	382

Viewing the Results of a New Workspace. ....	382
Understanding Differences Between Enterprise Resource Templates and Tenant Resource Templates. ....	384
Enabling or Disabling Built-in Resource Templates .....	384
Deleting Workspaces. ....	389
Managing Workspace Users After Deleting a Workspace. ....	390
Customizing Resource Templates. ....	390
Creating a Custom Resource Template .....	391
Resource Template Location and Files. ....	392
Resource Template Variables. ....	393
Creating a Model Using the Enterprise Resource Template. ....	394
Adding Customizations to the Custom Resource Template. ....	397
Exporting the Custom Resource Template. ....	398
Updating Resource Template Properties. ....	399
Removing the Model. ....	400
Understanding Access Control Templates .....	401
Developing Business Requirements for Server Access Control Templates. ....	402
Access Control Template Regular Expressions and Group ID Patterns. ....	403
Creating Access Control Templates. ....	403
Access Control Template Prerequisites. ....	404
Choosing an Access Control Template Creation Method. ....	412
Creating Access Control Templates by Copying and Pasting. ....	412
Creating Access Control Templates by Manual Configuration. ....	417
Creating a Template Model. ....	417
Creating and Registering Server Access Control Templates. ....	428
Testing the Combined Resource Template and Access Control Template Solution. ....	433
Assess Your Test Results. ....	439
Working With Message Templates .....	439
Understanding Message Template Text Strings. ....	440
<b>6. User Administration .....</b>	<b>443</b>
Using the Security Center .....	444
Managing Users .....	444

Understanding Users.....	445
Understanding User Name Requirements.....	446
Importing Users.....	448
Understanding User Import File Layout and Format Requirements.....	448
Understanding User Record Field Format Requirements.....	449
Understanding the Group Membership Report.....	453
Managing Groups .....	455
Understanding Groups.....	455
Workspace Groups.....	456
Basic Users.....	456
Advanced Users.....	456
Authors.....	456
Developers.....	457
Group Administrators.....	457
Infrastructure Groups.....	457
My_Workspace Group.....	457
Administrators Group.....	458
Anonymous Group.....	458
EVERYONE Group.....	459
Managers Group.....	459
SelfServiceDevelopers Group.....	459
Managing Roles .....	463
Privilege Categories.....	464
Migration Functionality and User Defined Roles (UDR).....	469
Managing Rules .....	470
Managing Private Resources .....	474
<b>7. Securing a TIBCO WebFOCUS Environment .....</b>	<b>477</b>
Information Assurance Best Practices .....	477
Documentation .....	478
Open Web Application Security Project (OWASP) .....	478
ReportCaster Settings .....	479
TIBCO WebFOCUS Reporting Server Security .....	479

Differentiating TIBCO WebFOCUS Reporting Server Access Control and IBFS Security .....	480
Differentiating Data Security and IBFS Security .....	481
Protecting TIBCO WebFOCUS Variables .....	481
TIBCO WebFOCUS Encryption Features .....	481
Default TIBCO WebFOCUS Encryption and AES Encryption.....	482
Configuring Encryption in the TIBCO WebFOCUS Client.....	483
<b>8. TIBCO WebFOCUS Change Management .....</b>	<b>487</b>
Understanding the Change Management Process .....	487
Creating a Change Management Package .....	489
Working With CM Zip Files.....	490
Including Collaborative Portals in a Change Management Package.....	491
Understanding Change Management Import Options.....	505
<b>A. Configuration Settings .....</b>	<b>511</b>
TIBCO WebFOCUS Client Configuration Files .....	511
Application Settings .....	513
Configuring Run With Different Connection Credentials.....	559
Configuring Solr Basic Authentication.....	572
TIBCO WebFOCUS Designer Properties .....	574
InfoAssist Properties .....	575
Enabling the Cache Through Global Preferences.....	584
InfoAssist Basic Properties.....	590
<b>B. Logging .....</b>	<b>591</b>
Daily Log and Trace File Maintenance .....	591
Understanding Audit Logs .....	592
Customizing the Audit Log Configuration.....	594
Understanding Security Events.....	603
Understanding Configuration Events.....	603
Understanding Content Events.....	604
Understanding Group Events.....	606
Understanding Library Access Events.....	607
Understanding Magnify Console Events.....	608
Understanding Ownership Events.....	614



Understanding ReportCaster Configuration Events. ....	615
Understanding ReportCaster Global Update Events. ....	616
Understanding Role Events. ....	617
Understanding Rule Events. ....	617
Understanding Sharing Events. ....	618
Understanding Sign-in Events. ....	619
Understanding User Events. ....	622
Understanding Monitor Logs ....	623
Understanding a Monitor Log Event. ....	623
Understanding the Monitor ID ....	627
Understanding Change Management Import and Export Logs ....	628
Export Package Created By Entry. ....	629
Understanding the Advanced Web Tools, BI Portal, Event, EclipseLink JPA, and ReportCaster Log ....	629
<b>C. Diagnostics .....</b>	<b>631</b>
Understanding All Clients Traces ....	631
Understanding Client Connector Traces ....	631
Understanding Monitor Log Traces ....	632
Understanding Web Security Traces ....	633
Understanding Web Services Traces ....	634
Understanding WFServlet Traces ....	634
<b>D. Privileges .....</b>	<b>635</b>
Basic Reporting ....	635
Advanced Reporting ....	638
Scheduling and Distribution ....	640
Application Development ....	643
Desktop Development ....	645
Group Administration ....	648
Administration ....	650
<b>E. Providing Data Source Security: DBA .....</b>	<b>653</b>
Introduction to Data Source Security ....	653
Implementing Data Source Security ....	654

Identifying the DBA: The DBA Attribute. ....	656
Including the DBA Attribute in a HOLD File. ....	657
Identifying Users With Access Rights: The USER Attribute. ....	657
Non-Overridable User Passwords (SET PERMPASS). ....	658
Controlling Case Sensitivity of Passwords. ....	660
Establishing User Identity. ....	661
Specifying an Access Type: The ACCESS Attribute ....	662
Types of Access. ....	663
Limiting Data Source Access: The RESTRICT Attribute ....	665
Restricting Access to a Field or a Segment. ....	668
Restricting Access to a Value. ....	670
Restricting Both Read and Write Values. ....	672
Controlling the Source of Access Restrictions in a Multi-file Structure ....	672
Adding DBA Restrictions to the Join Condition ....	676
Placing Security Information in a Central Master File ....	676
File Naming Requirements for DBAFILE. ....	681
Connection to an Existing DBA System With DBAFILE. ....	681
Combining Applications With DBAFILE. ....	682
Summary of Security Attributes ....	682
Hiding Restriction Rules: The ENCRYPT Command ....	684
Encrypting Data. ....	684
Performance Considerations for Encrypted Data. ....	685
Setting a Password Externally. ....	686
FOCEXEC Security ....	686
Encrypting and Decrypting a FOCEXEC. ....	686
<b>F. App Studio Custom Logon Templates .....</b>	<b>689</b>
How Logon Templates Work ....	689
Creating a Custom Template ....	692
Configuring App Studio to Support IBM Tivoli Access Manager WebSEAL ....	700
Additional WebSEAL Configuration Steps ....	705
Creating the jmt.conf File. ....	706
<b>G. Manipulating TIBCO WebFOCUS Variables .....</b>	<b>707</b>

Customizing TIBCO WebFOCUS Request Processing .....	707
TIBCO WebFOCUS Script and Configuration Files .....	709
TIBCO WebFOCUS Variables .....	710
TIBCO WebFOCUS Variable Table.....	710
TIBCO WebFOCUS Script Commands .....	710
TIBCO WebFOCUS Servlet Plug-in .....	715
CopyHTTPHeaderToWFVar Method.....	717
CopyWFVarToSessionVar Method.....	717
CopySessionVarToWFVar Method.....	719
CopyHTTPMethodToWFVar Method.....	720
CopyHTTPCookieToWFVar Method.....	720
Managed Reporting Internal Variables .....	723
HTTP Header Variables Available for Script Processing .....	725
<b>H. TIBCO WebFOCUS 8 Implementation for PCI Security Standards .....</b>	<b>727</b>
About the PCI Security Standards .....	727
Build and Maintain a Secure Network and Systems .....	728
Requirement 1: Install and maintain a firewall configuration to protect cardholder data..	728
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.....	730
Protect Cardholder Data .....	732
Requirement 3: Protect stored cardholder data.....	732
Requirement 4: Encrypt transmission of cardholder data across open, public networks..	732
Maintain a Vulnerability Management Program .....	732
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs.....	732
Requirement 6: Develop and maintain secure systems and applications.....	733
Implement Strong Access Control Measures .....	734
Requirement 7: Restrict access to cardholder data by business need to know.....	734
Requirement 8: Identify and authenticate access to system components.....	734
Requirement 9: Restrict physical access to cardholder data.....	735
Regularly Monitor and Test Networks .....	735

- Requirement 10: Track and monitor all access to network resources and cardholder data..... 736
- Requirement 11: Regularly test security systems and processes..... 737
- Maintain an Information Security Policy .....738
- Requirement 12: Maintain a policy that addresses information security for all personnel 738
- I. Replicating the TIBCO WebFOCUS Repository Database ..... 739**
  - Overview ..... 739
  - Understanding Database Replication Settings ..... 746
- J. Glossary ..... 751**
- Legal and Third-Party Notices ..... 759**

# TIBCO WebFOCUS Components and Deployment Options

---

TIBCO WebFOCUS® offers easy to use reporting, business analytics, and performance management tools, and a wide range of security integration options, empowering organizations with the business knowledge to make effective decisions and attain a competitive edge.

WebFOCUS® integrates with your existing network infrastructure by connecting your web and application servers to your operational data. The following topics describe the many ways you can configure the components so that they provide a seamless and secure environment for your application development and production environments.

**In this chapter:**

- ❑ [The TIBCO WebFOCUS Security Model](#)
  - ❑ [TIBCO WebFOCUS Components](#)
  - ❑ [TIBCO WebFOCUS Deployment Options](#)
- 

## The TIBCO WebFOCUS Security Model

The WebFOCUS security model enables an administrator to implement security at a granular level for every resource in the WebFOCUS Repository, if needed. User actions can be permitted for individual combinations of users and resources. Access privileges can be inherited from higher level folders, or an administrator can grant or deny access privileges directly to a specific group or user.

Highlights of the model include:

- ❑ Relational database storage for all content.
- ❑ Improved integration with ReportCaster.
- ❑ Single sign on for all mid-tier components.
- ❑ Multiple role capability.
- ❑ Improved integration with Software as a Service (SaaS) vendors.
- ❑ Granular delegation of administrative tasks.

- ☐ Improved security, including:
  - ☐ Security auditing.
  - ☐ Account policies.
  - ☐ Multiple authentication providers.
  - ☐ CSRF (Cross Site Request Forgery) filter to guard against CSRF attacks.
  - ☐ XSS (Cross Site Scripting) defenses to guard against XSS attacks.
  - ☐ Null byte injection filter to guard against null injection attacks.
  - ☐ Session fixation defenses to guard against session fixation attacks.
  - ☐ Customizable XFrameOptions HTTP response header to guard against clickjacking attacks.

To design security that fits the needs of your organization, you must consider several fundamental issues:

- ☐ **Authentication.** One of the primary decisions to make about any application is whether you need to know and control who is allowed to access it. Authentication is the process of confirming the identity of a user.
- ☐ **Authorization.** Once you have authenticated a user, the next step is to determine and then enforce an appropriate level of access. Authorization is the process of enforcing user privileges to control the access to resources and tools within an application.
- ☐ **Confidentiality.** Confidentiality ensures privacy, usually by encrypting information transmitted between or stored on components in an environment. Encryption may be weak or strong, and can be based on private or public encryption schemes. The decision regarding which data is sensitive is different for every organization.
- ☐ **Data Integrity.** Data integrity is the assurance that information cannot be altered without proper authorization.
- ☐ **Auditing.** Auditing tracks user access to tools and resources, and also logs important administrative actions, such as adding users to groups.

Questions that should shape your security policy include:

- ☐ What information will be stored in the WebFOCUS Repository?
- ☐ Who will need access to this information?

- ❑ What kind of access will each user need?
- ❑ Which tools should be available to each user?

## TIBCO WebFOCUS Components

The basic components of a WebFOCUS environment are:

- ❑ **Web Browser.** Enables access to a WebFOCUS environment using an HTTP or HTTPS connection to a web server, or an application server configured as a web server.
- ❑ **Web Server.** An optional component that supports a web agent and external authentication features, such as integrated Windows authentication and SiteMinder agents. The Web Server accepts requests for information from the web browser, and passes the requests to the application server. It also receives responses to requests from the application server, and returns them to the web browser. (Configurations that do not include a web server use the application server for these tasks.)
- ❑ **Load Balancer.** An optional component that supports installations that maintain multiple servers or clusters by distributing client requests to servers. The Load Balancer receives incoming requests from the web browser and forwards them to the different application servers for processing.
- ❑ **Application Server.** Handles all application operations between users and business applications or databases. Frequently, application servers also function as web servers. One of its functions is to communicate with the database. The Application Server can also connect to the TIBCO WebFOCUS® Reporting Server or the database server depending upon the nature or the request.
- ❑ **TIBCO WebFOCUS® Client.** Controls the flow of information between the web server and WebFOCUS® Reporting Server. The WebFOCUS® Client runs underneath the Application Server. It accesses the Repository DBMS or the Reporting Server to pass requests from the web server and passes the results from these components back to the web server. The WebFOCUS client includes the following components:
  - ❑ **Business Intelligence Portal (BI Portal).** Enables end users to access WebFOCUS reports through a professional, easily branded web interface.
  - ❑ **Managed Reporting.** Establishes a WebFOCUS environment for creating and viewing reports. An important function of Managed Reporting is allowing administrators to create users, define their access rights, and create end-user reports. Users access Managed Reporting to create and view reports using data to which an administrator has granted them access.

- ❑ **ReportCaster.** Provides advanced scheduling and distribution capabilities for WebFOCUS reports (self-service and Managed Reporting) and alerts, as well as independent files and URLs.
- ❑ **Report Library.** Stores reports, files, and the contents of URLs distributed by ReportCaster.
- ❑ **Open Portal Services.** Supports integration between Managed Reporting and popular portal products.
- ❑ **TIBCO WebFOCUS Reporting Server.** Holds metadata for the data sources WebFOCUS can access, and controls access to those data sources. It is responsible for executing the queries against these data sources and retrieving and formatting the query results, which it then passes to the WebFOCUS Client. It provides multiple data adapters that give users access to data in many different types of data sources.
- ❑ **WebFOCUS Database Repository Server.** Is the relational database system that contains WebFOCUS content, such as reports, charts, queries, users, groups, roles, ReportCaster schedules, requests, images, library schedules, saved deferred reports, and other items.

You can add the following optional product to your WebFOCUS environment:

- ❑ **TIBCO WebFOCUS® App Studio.** Enables you to develop WebFOCUS applications using a Windows-based development environment.

## TIBCO WebFOCUS Deployment Options

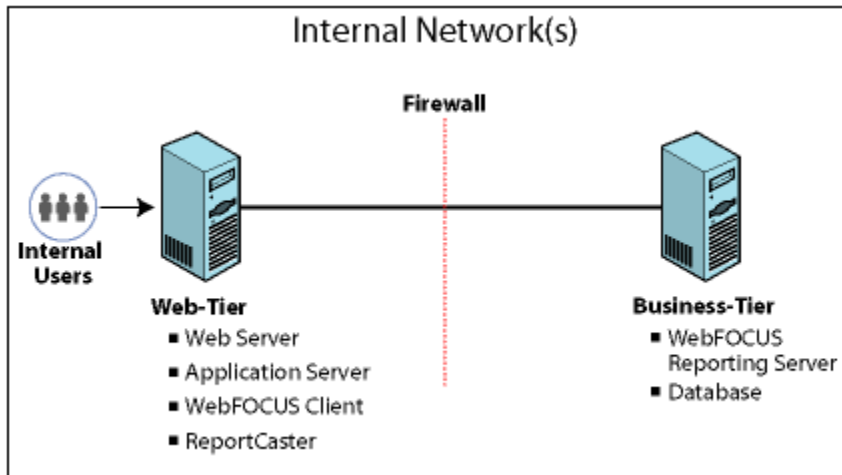
The WebFOCUS components can be deployed in several different ways so that you can plan your installation according to your needs.

### Basic Internal Deployment Pattern

Internal users (on a trusted network) access WebFOCUS using a standard installation. The WebFOCUS Client and Reporting Server can be installed on the same host or on two hosts connected by a network. The ReportCaster Distribution Server is typically installed on the same host as the WebFOCUS Client to simplify configuration and administration.



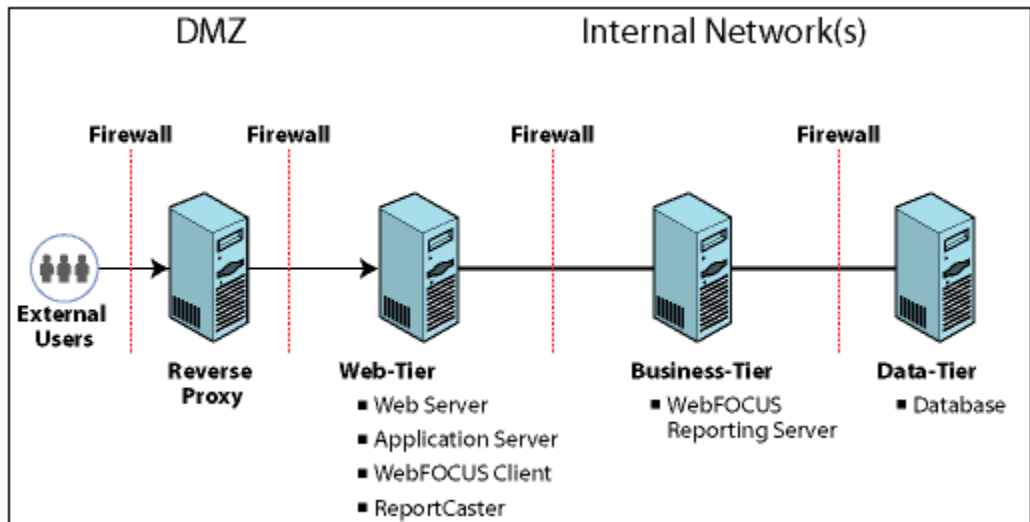
The database can be on the business tier or on a separate data tier. If on a separate machine, it can optionally be behind a firewall, if necessary. In this case, communication between the tiers can be implemented using a WebFOCUS Reporting Server hub-stub configuration or the database connection software of the vendor.



### Basic External Deployment Pattern

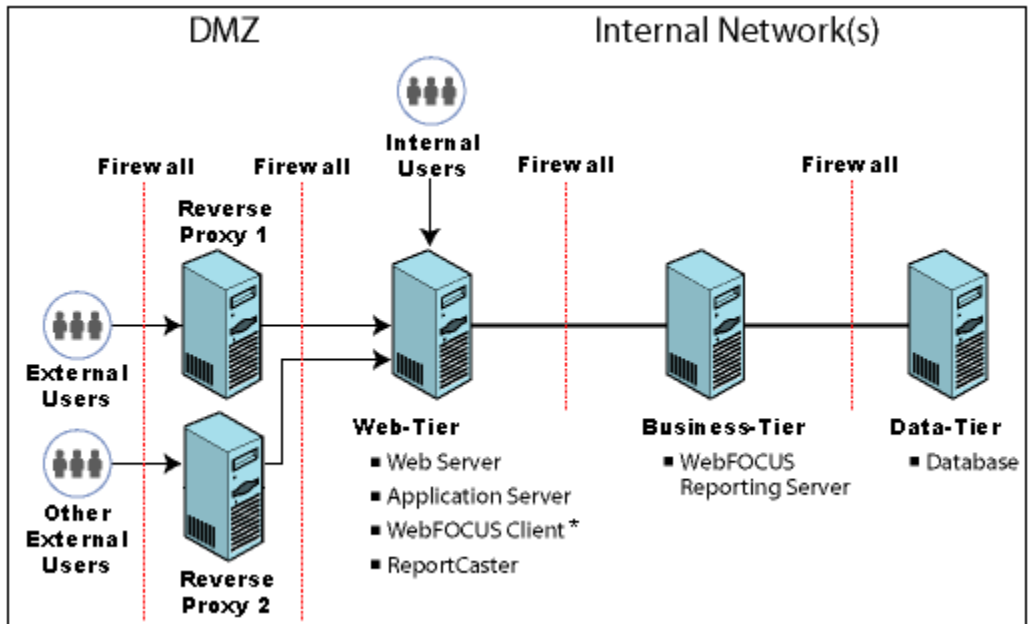
When external users access WebFOCUS, you can optionally configure them to interact with a reverse proxy server. A reverse proxy server is a web server that acts as an intermediary between the external network and the web server on which WebFOCUS is installed. Each component can optionally be protected by a firewall.

With a reverse proxy server, external users think that they are directly accessing WebFOCUS. However, the proxy server actually receives incoming HTTP requests and forwards them to the web server on which WebFOCUS is installed, adding an additional layer of security.



## Mixed Deployment Pattern

WebFOCUS supports multiple entry points into a single WebFOCUS installation. For example, there may be both external users going through a reverse proxy server, and internal users directly accessing the web tier. There may also be two or more reverse proxy servers for different user communities, as shown in the following image.





## Configuring the TIBCO WebFOCUS Reporting Server

---

This topic explains how to configure the TIBCO WebFOCUS Reporting Server for use with ReportCaster and the WebFOCUS Client. Communication with the WebFOCUS Reporting Server is required for many different purposes, including:

- ☐ To authenticate users against an external source, including Active Directory and LDAP directories.
- ☐ To obtain group membership information to perform user authorization.
- ☐ To run reports online.
- ☐ To run reports deferred.
- ☐ For ReportCaster, to submit reports to run.

### In this chapter:

- ☐ [TIBCO WebFOCUS Reporting Server Security Modes](#)
  - ☐ [IP Restriction Filtering](#)
  - ☐ [Configuring a Security Provider on the TIBCO WebFOCUS Reporting Server](#)
  - ☐ [Configuring Trusted Connections](#)
  - ☐ [Configuring TIBCO WebFOCUS for SSL](#)
  - ☐ [TIBCO WebFOCUS Reporting Server Profiles](#)
- 

## TIBCO WebFOCUS Reporting Server Security Modes

WebFOCUS Reporting Server security runs in one of the following modes:

- ☐ **PTH (internal).** Access to the WebFOCUS Reporting Server is controlled by authenticating against the user list defined at the configuration level (user IDs and passwords have to be configured in the admin.cfg file). When security is set to PTH, there is no impersonation or authentication at the level of the operating system, and all server processes run as a single user ID from the operating system point of view. This is the default authentication mode.

❑ **LDAP.** An external directory service authenticates users. User and group profiles control access to resources. The user credentials from the WebFOCUS Client connection are authenticated through the established directory services. Impersonation is not applicable for this security mode.

❑ **OPSYS.** Each user is defined in the operating system on which the WebFOCUS Reporting Server is running. The WebFOCUS Reporting Server uses operating system services to authenticate connecting users, impersonate them, and control access to resources like files and DBMS objects. User authentication by the operating system protects access to the Reporting Server browser interface administrative functions.

The native security system of the operating system authenticates user credentials. The WebFOCUS Reporting Server then allocates a data access agent which fully impersonates that user, so that the operating system governs access to files or other objects.

❑ **DBMS.** Users are authenticated using a list of user IDs stored in a relational data source. There is no impersonation or authentication by the operating system security for any user credentials supplied by WebFOCUS. Instead, the users may be defined on the DBMS server or the WebFOCUS subserver. This technique is called *password pass-through*, as user IDs and passwords supplied by the WebFOCUS Client are passed to the next level for authentication.

❑ **CUSTOM.** The user is authenticated by a custom procedure.

❑ **OFF.** The user is not authenticated by the built-in WebFOCUS Reporting Server security, and all agents created by the WebFOCUS Reporting Server will run with the security profile of the user who started the WebFOCUS Reporting Server. A security plug-in can be used as an alternative means for authenticating the user.

**Note:** WebFOCUS Reporting Server roles and templates are independent of roles and templates in the WebFOCUS Client, but perform similar functions. A user can be a Server Administrator on the WebFOCUS Reporting Server while being a basic user, or not existing, in the WebFOCUS Client. While you are configuring a security provider, you do not need to configure any of the Server roles and templates except the Server Administrator role. For more information on WebFOCUS Reporting Server roles and templates, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

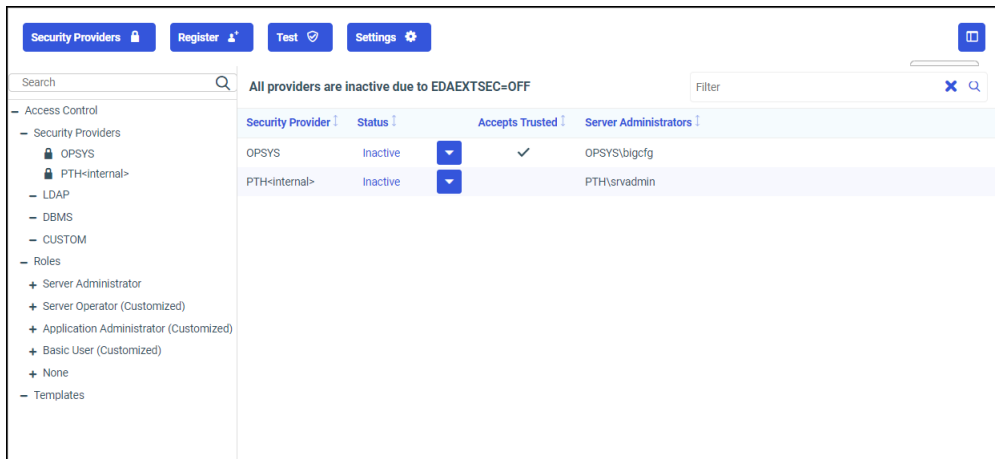
To create or edit a security provider, double-click on the appropriate security node. Configuration options will appear in the main page. Alternatively, right-click on the security mode and select *New* to create a new provider or *Properties* to modify an existing provider. If you select *Properties* for a security node which has no providers configured, the main page displays the options for configuring a new provider.

The Access Control tab displays the Manage Providers page when you first open it. You can always return to this page by double-clicking the Security Providers folder or by clicking the *Manage Providers* button in the ribbon. The Manage Providers page lists the providers currently configured, their status, their Server Administrators, and whether or not they accept trusted connections. It also lists the current Server Administrator.

The security behavior of the agent process of the user varies depending on your WebFOCUS Reporting Server security setting. For more information, see the *TIBCO WebFOCUS Reporting Server Administration* manual.

## TIBCO WebFOCUS Reporting Server Browser Interface

You configure security providers by using the *Access Control* tab of the Reporting Server browser interface, which is shown in the following image.



The Access Control tab consists of the following elements:

- ❑ A navigation pane for selecting security providers, templates, and roles. For more information about the security providers listed on this page, see [TIBCO WebFOCUS Reporting Server Security Modes](#) on page 25.
- ❑ A main page for configuring or viewing the settings for the selected provider, template, or role.

## Navigating to the Reporting Server Browser Interface

To open the Reporting Server browser interface directly from the browser address bar:

- ❑ Type the following URL:

`http(s)://host:port`

where:

`host`

Is the name or IP address of the host used to access the WebFOCUS Reporting Server.

For example:

`server01.ibi.com`

`port`

Is the number of the port on which the WebFOCUS Reporting Server listens.

For example:

`8121`

If you are prompted to sign in, type the credentials of a Server Administrator who has the privilege to manage the WebFOCUS Reporting Server.

**Note:** If you have trouble contacting the WebFOCUS Reporting Server, or if you are running your WebFOCUS Reporting Server with security and need information on the requirements and options associated with the security mode you are using, see the *TIBCO WebFOCUS® Reporting Server Administration* technical content for more information.

If you are already signed in, you can open the Reporting Server browser interface by selecting one of the following options from the left side navigation pane on the Hub.

- ☐ *Application Directories* to open the Application Directories page.
- ☐ *Management Center* and then selecting one of the following links under *Server Administration*.
  - ☐ *Server Preferences* to open the Server Preferences page.
  - ☐ *Access Control* to open the Access Control page.
  - ☐ *Server Workspaces* to open the Workspaces page.
  - ☐ *Resource Management* to open the Resource Management page.
  - ☐ *Scalability page* to open the Scalability page.

**Note:** You can also select *Administration Console* under *Client Administration*, if you want to open the Reporting Server browser interface from the Administration Console.



To open the Reporting Server browser interface from the WebFOCUS Home Page:

- ❑ On the banner, select *Settings* and then select *WebFOCUS Server*.

Or

- ❑ On the banner, select the *Plus* button and then select *Prepare and Manage Data*.

To open the Reporting Server browser interface from the Legacy Home Page:

- ❑ In the Resources tree, expand the *Reporting Servers* node. Right-click the node for the WebFOCUS Reporting Server you want to work with, and then click *Reporting Server Console*.

Or

- ❑ On the BI Portal menu bar, click *Administration*, and then click *Administration Console*. Follow the steps to open the Reporting Server browser interface from the Administration Console.

To open the Reporting Server browser interface from the Administration Console:

- ❑ On the Configuration tab, expand the Reporting Servers folder and then expand the Server Connections folder. Right-click the WebFOCUS Reporting Server you want to work with, and then click *Reporting Server Console*.

If you are prompted to sign in, type the credentials of a Server Administrator who has the privilege to manage the WebFOCUS Reporting Server.

## IP Restriction Filtering

It is strongly recommended that you restrict the IP addresses that are allowed to connect to the WebFOCUS Reporting Server for service requests. Limiting the connections to the IP addresses required for the TCP Listener (LST\_TCP) and the HTTP Listener (LST\_HTTP) prevents unauthorized users from making use of the trusted connection between the WebFOCUS Reporting Server and the WebFOCUS Client.

The IP addresses that are allowed for incoming connections are defined by the RESTRICT\_TO\_IP keyword in the WebFOCUS Reporting Server communications configuration file (odin.cfg). If the odin.cfg file does not contain the RESTRICT\_TO\_IP keyword, any IP address is permitted. For more information about using the RESTRICT\_TO\_IP keyword, see *Listeners and Special Services* in the *TIBCO WebFOCUS® Reporting Server Administration* manual.

## Configuring a Security Provider on the TIBCO WebFOCUS Reporting Server

When you configure pre-authentication, external authentication, or external authorization, the WebFOCUS Client uses the security providers configured on the WebFOCUS Reporting Server (WFRS) to query the external source for information about users. The security provider may be LDAP or Active Directory, or it may use a custom method of authentication or authorization, such as authenticating users to a web service or authorizing them based on information stored in a table in a relational database management system (RDBMS).

The WebFOCUS Reporting Server supports multiple concurrent security providers. You must always configure a primary provider and may optionally configure one or more secondary providers. It is recommended that you authorize WebFOCUS users through the primary provider.

When you install the WebFOCUS Reporting Server, PTH (internal authentication) is automatically configured as the default security provider. In order to see this default configuration in the Reporting Server browser interface, you must start the WebFOCUS Reporting Server with the Start Security ON command. You can use the PTH Server Administrator that is automatically created during installation to configure the external sources that you plan to use for pre-authentication or external authentication. Once you have configured your preferred method of authentication, it is recommended that you configure PTH as a secondary security provider. This ensures that you can access the Reporting Server browser interface even if the primary provider is unavailable.

PTH can also be useful as the security provider for the WebFOCUS Reporting Server service account used to communicate with the WebFOCUS Client. Governance policies often require that passwords in the external source be changed on a regular basis and never be stored in configuration files, prohibiting the use of a non-expiring password for an account that belongs to the primary service provider. To avoid the necessity of managing updates to the service account password, you can specify a PTH account that does not exist in the external source and give the account the Server Administrator role and a password that is set never to expire.

**Note:** When you do not specify the provider for a user account, it is treated as an account from the primary provider. To use multiple WebFOCUS Reporting Server security providers for authentication, prefix the WebFOCUS user ID with the secondary security provider name for any individuals associated with it. For example, if the WebFOCUS Reporting Server has two LDAP providers, a primary provider named ldap01 and a secondary provider named ldap02, then the user accounts ldap01\user1 and ldap02\user2 must be created in WebFOCUS as user1 and ldap02\user2, respectively.

## Configuring an LDAP or Active Directory Security Provider on the TIBCO WebFOCUS Reporting Server

To configure a new LDAP or Active Directory security provider, you create the provider, set up user search and group search, and configure the security provider to allow trusted connection from other applications. You may also want to change its status to primary provider or secondary provider, since new providers are automatically configured as inactive.

**Note:** You can change properties by right-clicking the provider name to access the Security Configuration pane.

### **Procedure:** How to Configure an LDAP Security Provider on the TIBCO WebFOCUS Reporting Server

1. Open the Access Control page of the Reporting Server browser interface. If prompted, sign in with a valid Server Administrator User ID, Password. and select a Security Provider, if the Security Provider list appears on the Sign in page.

2. Under Security Providers, right-click *LDAP*, and then click *New*.

Or

On the banner, select *Security Providers*, *New Provider*, and *LDAP*.

The LDAP Security Configuration tab opens.

3. Click *Continue*, and then type your provider name in the LDAP\_PROVIDER field.

This name appears as the vendor name in the Access Control navigation pane.

4. Complete the Connection section fields as follows:

- ☐ In the `ldap_host` field, type the name of the LDAP host.
- ☐ In the `ldap_port` field, accept the default value or type the dedicated LDAP port number.
- ☐ In the Security list, accept the *Anonymous or Windows security - NEGOTIATE* option, which appears by default, if you use an anonymous bind or if you use a Windows-specific API to authenticate your connection to the LDAP Security provider.

Select *Explicit* if you use an explicit bind to authenticate your connection to the LDAP Security provider. This bind is performed under the account that is defined by the configuration parameters `ldap_principal` and `ldap_credentials`. Type the name of the service account in the `ldap_principal` field and its nonexpiring password in the `ldap_credentials` field.

**Note:** The Explicit option is recommended when integrating the WebFOCUS Reporting Server with WebFOCUS Client security.

- ☐ In the `ldap_search_timeout` field, accept the default value of 60 seconds or type the number of seconds duration for LDAP searches.

5. Click *Next*.

The page refreshes and expands the User Search section. The Group Search, Trusted Connections, and Environment sections also appear in collapsed form.

6. The WebFOCUS Reporting Server connects to the user directory and determines its vendor and version number, then fills in the typical default values for that directory in the User Search window and the Group Search window.

**Note:**

- ☐ If the fields for a specific window are not visible, click the down arrow on the separator bar for that window to open.

- ☐ If your directory does not use the default values for its type, consult your AD or LDAP administrator for the appropriate settings.

7. When the values for the User Search configuration and the Group Search configuration are entered, click *Test User Authentication*.

The Testing LDAP Security dialog box opens.

8. Type the LDAP user name and password of any account in the external directory, then click *Continue*.

If the credentials are successfully authenticated, the WebFOCUS Reporting Server displays the list of LDAP or Active Directory groups found for the user. If you are using a custom attribute, the WebFOCUS Reporting Server displays the attribute values for this user.

If the credentials are not successfully authenticated, you receive an error message that provides details.

**Note:** The test typically finishes within a second. If the results are slow to appear, check with your directory and network administrators to ensure that the connection, user, and group configuration settings are optimal for your environment.

9. Close the Test Results dialog box. If you would like to configure this security provider to accept trusted connections, click the *Trusted Connections* separator bar and set `trust_ext` to `y`.

10. Click *Save*.

The Activate Providers pane appears. The new provider appears in the list of security providers as an inactive provider.

## Understanding LDAP Security Provider Properties

You must specify connection properties, user properties, and group properties for each LDAP provider configured.

**Reference:** Understanding LDAP Connection Properties

### LDAP\_PROVIDER

Specifies a name for the LDAP provider.

### ldap\_host

Is a host identifier consisting of a host name or an IPv4 dotted string representing the IP address of the host running the LDAP server.

Alternatively, the entry for the ldap\_host field may consist of a list of space-delimited host identifiers. Each host identifier may include a trailing colon and port number. When more than one host identifier is specified, each host identifier will be contacted in turn until a successful connection is established.

The following examples are all valid values for the ldap\_host setting:

```
directory.example.com
192.0.2.0
directory.example.com:1050 people.catalog.com 192.0.2.0
```

### ldap\_secure\_connection

Specifies whether the WebFOCUS Reporting Server uses a Secure Socket Layer (SSL) connection to the LDAP server. The default value is No.

An LDAP security provider supports SSL API calls to establish an SSL/TLS connection. Using Server authentication only, the WebFOCUS Reporting Server initiates API calls to verify that the LDAP server being connected to is the same server that provided certification.

If you select IBM, Sun, or Novell as your ldap\_lib\_vendor and specify an SSL connection, additional options appear:

- ☐ For Sun and IBM, ldap\_ssl\_certificate appears.

- ❑ For Novell, `ldap_ssl_certificate` and `ldap_ssl_certification_encoding` appear.

### **ldap\_ssl\_certificate**

Specifies the LDAP attribute that the API uses to establish the SSL/TLS connection. Values depend on the LDAP vendor, as follows:

- ❑ **Novell API.** Specifies the file name, including the path, of the Trusted Root Certificate that the LDAP server provides for authentication.
- ❑ **Sun/Netscape API.** Specifies the path to `cert7.db`, the Netscape certificate database, excluding the file name, that the LDAP server provides for authentication.
- ❑ **IBM API.** Specifies the file name, including the path, for `ldapkey.kdb` (the IBM database file that the LDAP server provides for authentication). The `ldapkey.sth` password stash file should be in the same directory.

**Note:** SSL requires Global Security Kit (GSK) libraries in addition to IBM LDAP client libraries. GSK must be installed on Windows machines.

- ❑ **Microsoft API.** Ignores the `ldap_ssl_certificate` configuration, which is not used in an Active Directory. The server certificate should be installed in a certificate store.

### **ldap\_ssl\_certification\_encoding**

For Novell, specifies the standard used to encode the certificate. Encryption and file format depend on API vendor specifications. The options are B64 and DER.

### **ldap\_port**

Is a positive integer that defines the TCP port number used to connect to the LDAP server. Note that `ldap_port` is ignored for any host identifier which includes a colon and port number. The default port is 389 or 636 (for SSL connections).

### **security**

Determines the type of bind used.

- ❑ **Anonymous or Windows security - NEGOTIATE**

No credentials are required. This is the default value.

If the Server is installed on a Windows machine, the bind defaults to NEGOTIATE when this option is selected. Otherwise, the bind is anonymous.

In negotiation, a Windows-specific API authenticates WebFOCUS Reporting Server connections against Active Directory. The bind is performed by the current Windows user (the Windows account that started the Server). The Windows machine that hosts the WebFOCUS Reporting Server should be in the same domain as the Active Directory server.

#### ☐ **Explicit**

The bind is performed by the account defined by the `ldap_principal` and `ldap_credentials` settings.

#### **Note:**

- ☐ The Explicit option is recommended when integrating the WebFOCUS Reporting Server with WebFOCUS Client security.
- ☐ When connecting to Active Directory using Explicit or Anonymous or Windows security - NEGOTIATE, the default value for `ldap_user_attribute` is `sAMAccountName`. You can customize this as desired.

#### **ldap\_principal**

Specifies the name of the service account.

**Note:** This setting is visible only when the security setting is Explicit.

#### **ldap\_credentials**

Specifies the password of the service account. It is recommended that this password be nonexpiring.

**Note:** This setting is visible only when the security setting is Explicit.

#### **ldap\_search\_timeout**

Specifies how long (in seconds) LDAP searches can last before they time out.

#### **ldap\_referrals**

Specifies if child domains should be searched following the referrals returned by the root domain. The default value is No.

#### **ldap\_gghost**

Specifies the Active Directory Global Catalog host name.

#### **ldap\_gcport**

Specifies the Active Directory Global Catalog port. Note that `ldap_gcport` should be chosen in pair with `ldap_port`. Either a non ssl-pair(389/3268) should be used or an ssl pair(636/3269). If a value is assigned to this field, it must be a positive integer.

If you select OpenLDAP on LINUX, the additional properties of `ldap_libldap` and `ldap_liblber` also appear. Both properties specify the names of OpenLDAP libraries that the Server loads at run time. The path to the libraries must be available to the Server at run time, when you will be prompted to specify the library names. If you do not supply names at that time, the library names entered in `ldap_libldap` and `ldap_liblber` will be used.

**Reference:** Understanding LDAP User Properties

**ldap\_user\_base**

Specifies the DN of the entry that serves as the starting point for the LDAP server search for users.

**ldap\_user\_scope**

Specifies where the WebFOCUS Reporting Server starts to search through the LDAP directory for users. Options are:

**Subtree.** Search everything under the base DN. This is the default value.

**Onelevel.** Search only entries one level down from the base DN.

**Base.** Search only the base DN.

**ldap\_user\_class**

Specifies the object class used when searching for user entries.

**ldap\_user\_attribute**

Specifies the attribute used when searching for user entries. A common reason to change the default value is to allow users to sign in with an email address instead of a user ID. To do this, you would set the `ldap_user_attribute` to `mail` or `userPrincipalName` (if this corresponds with the name of the appropriate attribute in your directory).

**ldap\_user\_group\_attribute**

Specifies the attribute used to identify a group in a user object.

**ldap\_user\_description**

Specifies the attribute whose value contains the description of an object (user, group).

**ldap\_user\_email**

Specifies the attribute that contains the email address of the user.

`ldap_user_class`, `ldap_user_attribute`, `ldap_group_class`, `ldap_group_attribute` are parameters that form a search filter. The search filter standard syntax conforms to the following structure:



```
(&(Property_Name=Property_Value)(Property_Name=Property_Value))
```

If you change the value of the `ldap_user_class` and `ldap_group_class` parameters to an asterisk (\*), the search filter syntax can be reduced to the following simplified form (although group support will not work properly):

```
(Property_Name=Property_Value)
```

By specifying an asterisk for these parameters, you achieve a simplified search filter syntax, but disable group support.

### **Reference: Understanding LDAP Group Properties**

#### **ldap\_group\_base**

Specifies the DN of the entry that serves as the starting point for the LDAP server search for groups. `ldap_group_base` consists of name-value pairs separated by commas.

#### **ldap\_group\_scope**

Specifies where the WebFOCUS Reporting Server starts to search through the LDAP directory for groups. Options are:

**Subtree.** Search everything under the base DN. This is the default value.

**Onelevel.** Search only entries one level down from the base DN.

**Base.** Search only the base DN.

#### **ldap\_group\_class**

Specifies the object class used when searching for group entries. The default value for LDAP is `groupofuniquenames`. The default value for Active Directory is `group`.

#### **ldap\_group\_attribute**

Specifies the attribute used to identify the name of the group. The default is `cn`.

#### **ldap\_member\_attribute**

Specifies the attribute used to identify users in a group. The default value is `uniqueMember`. The default value for Active Directory is `Member`.

#### **ldap\_nested\_groups**

Enables LDAP nested groups support. The default value is `No`, which disables nested group support.

### **ldap\_group\_description**

Contains additional information about the ldap group.

## **Configuring a Custom RDBMS Security Provider on the TIBCO WebFOCUS Reporting Server**

User information can be retrieved from a relational database management system (RDBMS). For example, you may want to retrieve email addresses, descriptions, and user authorizations from an existing database, rather than re-creating them in WebFOCUS. The information can be retrieved with SQL queries or with SQL stored procedures, but in either case, you create custom FOCUS procedures to get the information.

External authorization from an RDBMS table requires two FOCUS procedures. A third procedure is required if you will be authenticating users against information in the RDBMS as well. If the RDBMS does not contain user authentication information, configure the WebFOCUS Client to pre-authenticate users to identify them for external authorization. For more information about pre-authentication, see [Pre-Authentication](#) on page 234.

To enable the custom server security provider, you need to provide code that allows the WebFOCUS Reporting Server to perform the following tasks:

- ☐ Authenticate users based on user ID and password.
- ☐ Obtain all groups for a user.
- ☐ Obtain all groups in the system.
- ☐ Obtain all users for a group and all users in the system.

The files necessary to configure a sample SQL security provider on the Reporting Server are available at:

[techsupport.informationbuilders.com/tech/wbf/v8templates/wbf\\_8\\_server\\_custom\\_provider.html](http://techsupport.informationbuilders.com/tech/wbf/v8templates/wbf_8_server_custom_provider.html)

This page also includes information about the format the procedures must use when returning information.

Synonyms used by custom provider procedures should be moved to the directory EDACONF/catalog/custom. The WebFOCUS Reporting Server will protect adapter connections used by custom procedures by denying access to these connections by users who are not Server Administrators.

### **Procedure: How to Configure a Custom RDBMS Security Provider on the TIBCO WebFOCUS Reporting Server**

1. Open the Access Control page of the Reporting Server browser interface. If prompted, sign in with a valid Server Administrator User ID, Password. and select a Security Provider, if the Security Provider list appears on the Sign in page.

2. In the Access Control navigation pane, under Security Providers, right-click *CUSTOM*, and then click *New*.

Or

In the banner, select *Security Providers*, *New Provider*, and *CUSTOM*.

The CUSTOM Security Provider Configuration tab opens.

3. Type the custom security provider name in the CUSTOM\_PROVIDER field.

**Note:** We recommend that this name be all lowercase.

4. Specify the procedures that the WebFOCUS Reporting Server will use to retrieve information.
  - a. If the custom provider will support authentication, type the fully qualified name of the procedure that will authenticate users in the cust\_authenticateuser box, for example, \_edaconf/catalog/custom/wfsqlauthn. If WebFOCUS will be pre-authenticating users, leave the box blank.
  - b. Type the fully qualified name of a procedure that will return information about users in the cust\_usersbygroup box, for example, \_edaconf/catalog/custom/wfsqlusers.
  - c. Type the fully qualified name of a procedure that will return information about groups in the cust\_groupsbyuser box, for example, \_edaconf/catalog/custom/wfsqlgroups.
  - d. In the cust\_service list, click the WebFOCUS Reporting Server data service under which the procedures that return user information will run.
  - e. To configure this security provider to accept trusted connections, click y in the trust\_ext list.
5. Click *Test* and enter the name and password of any user whose information is stored in the database, then click *Test* again.

If the procedure retrieves the information successfully, the WebFOCUS Reporting Server responds that the user information is valid.

If the credentials are not successfully authenticated, an error message provides details.

**Note:** The test typically finishes within a second. If the results are slow to appear, check with your directory and network administrators to ensure that the connection, user, and group configuration settings are optimal for your environment.

6. Close the Test Results dialog box and click *Save*.

The Activate Providers pane appears. The new custom provider appears in the list of security providers as an inactive provider.

## **Reference: Custom Security Provider Properties**

When you configure a new custom security provider, you enter values for the following properties:

### **CUSTOM\_PROVIDER**

Specifies a name for the custom provider. By default, this setting displays the value `custnn`

Where:

*nn*

Is the two-digit sequence number of the provider.

### **cust\_authenticateuser**

Is the name of the procedure that authenticates users.

If you prefer, you can specify a default Server Administrator user ID and password to use when connecting to the WebFOCUS Reporting Server, instead of using an authentication procedure.

For information about creating an authentication procedure, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

### **cust\_usersbygroup**

Is the name of the procedure that returns the list of all users or, if the group name is passed to the procedure, the list of all users in the group.

For information about creating a procedure that returns users, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

### **cust\_groupsbyuser**

Is the name of the procedure that returns the list of all groups or, if a user ID is passed to the procedure, the list of all groups for the user ID. For information about creating a procedure that returns groups, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

### **cust\_service**

Is the name of the WebFOCUS Reporting Server data service under which the procedure used to retrieve user information runs. This can be a service that already exists or a custom service you create in the Data Services tab.

**cust\_hashpsswr**

Specifies whether the custom provider requires the use of a hash password to authenticate the connection. The default value is no.

**trust\_ext**

Specifies whether the WebFOCUS Reporting Server accepts trusted connections. The default value is no.

## Changing the Security Provider Configuration

A Server security provider can be assigned a primary, secondary, or inactive status. Only one security provider can be identified as a primary security provider. All other active security providers are identified as secondary. Any other security providers that are configured but not in use are inactive. When you do not specify a security provider for a user account, it is treated as an account from the primary provider.

When you change the status of the primary security provider, one of the other secondary security providers must be identified as the new primary security provider. If you do not select a new security provider to replace the existing primary provider the WebFOCUS Reporting Server identifies a new primary security provider automatically.

When changing security providers, we recommend that you always retain PTH<Internal> as a secondary security provider. This practice ensures that administrators can obtain access to the WebFOCUS Server, even if the primary security provider becomes unavailable.

We also recommend that you maintain a backup copy of the current version of the admin.cfg file, located in *drive:\ibi\profiles\*. This file contains PTH user information. You can use the backup copy to restore the PTH security provider if the main admin.cfg file becomes corrupted.

### **Procedure:** How to Register a User Account as a Server Administrator

WebFOCUS registers a Server Administrator account for the PTH (Internal) security provider during installation. You may wish to register additional users or groups as Server Administrators, either for those providers or for other providers you add later.

At least one of the active security providers in your configuration must have a registered Server Administrator account. However, you can designate any security provider to be the primary security provider even if no Server Administrator account is registered to it.

1. Open the Access Control page of the Reporting Server browser interface. If prompted, sign in with a valid Server Administrator User ID, Password. and select a Security Provider, if the Security Provider list appears on the Sign in page.
2. On the Access Control page, select *Register* and *Register User* to open the User Registration tab, as shown in the following image.

Activate Providers X User Registration X

☐ Manual ☒ Import From Provider

Only 10000 multiple users can be registered together at the same time in the next page, please use filter to limit the number.

Security Provider OPSYS

☒ Filter for multiple users

User ID Sample: \*abc\*

E-Mail Sample: \*abc\*

Next

3. Select *Manual* to open the manual version of the User Registration tab, as shown in the following image.

Activate Providers X User Registration X

☒ Manual ☐ Import From Provider

Security Provider OPSYS

User

Domain

Description

E-Mail

Inherit Privileges from Server Administrator

Optional password for scheduled runs or effective server administrator ONLY

Password

Confirm Password

Register

4. Select the Security Provider to which the new Server Administrator will be assigned.  
The page refreshes to conform to the layout for your selected provider. This layout is the same for each provider with a few minor variations as noted in the following steps.

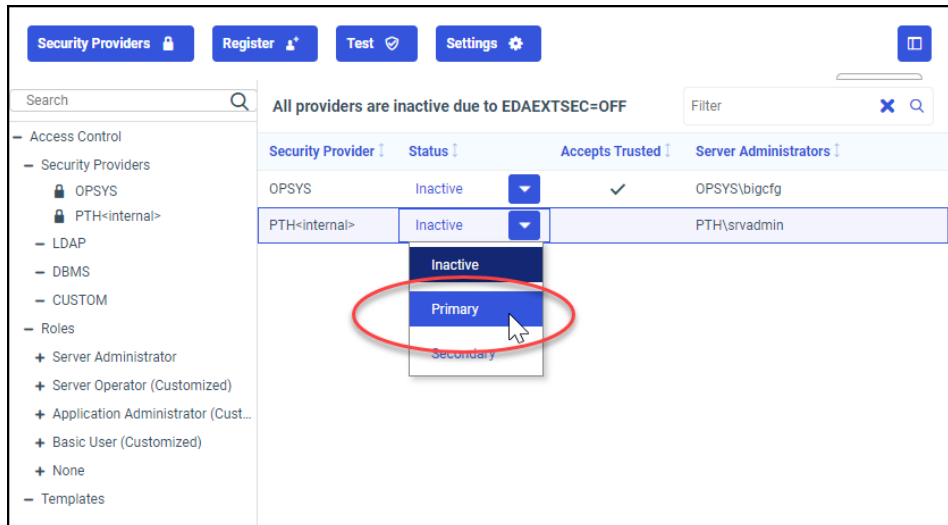
5. Enter the User ID of the new Server Administrator.  
**Note:** Use the *domain name\user ID* format if required.
6. If you selected the OPSYS Security Provider, select a Domain name for the user.
7. Enter an optional Description for the Server Administrator if you wish.
8. Enter the email address where notifications for this user are to be delivered.
9. Accept the default value of Server Administrator in the *Inherit Privileges from* list.  
 Select a different Server Role only if required to do so. For more information about Server Roles, see the *Server Administration* technical content.
10. If you selected the PTH<Internal> security provider, enter a password for this administrator in the Password and Confirm Password fields. If you selected a different security provider, this password is optional.  
**Note:** The WebFOCUS Reporting Server uses this password when conducting scheduled report distribution runs.
11. When your configuration is complete, select *Add and Register*, in the PTH<Internal> Security Provider version of the dialog box, or select *Register*, in any other version.
12. When you receive a message saying the New User will be added, select *OK*.
13. After the User Registration page refreshes, confirm that the ID and additional information of the newly-registered user appears on the page.

### **Procedure:** How to Configure a New Primary Security Provider

**Before you begin:** Ensure that you have created a security administrator for the new primary security provider as described in [How to Register a User Account as a Server Administrator](#) on page 41. You will be unable to access the Reporting Server browser interface after designating a new primary security provider if you do not have an administrator for it.

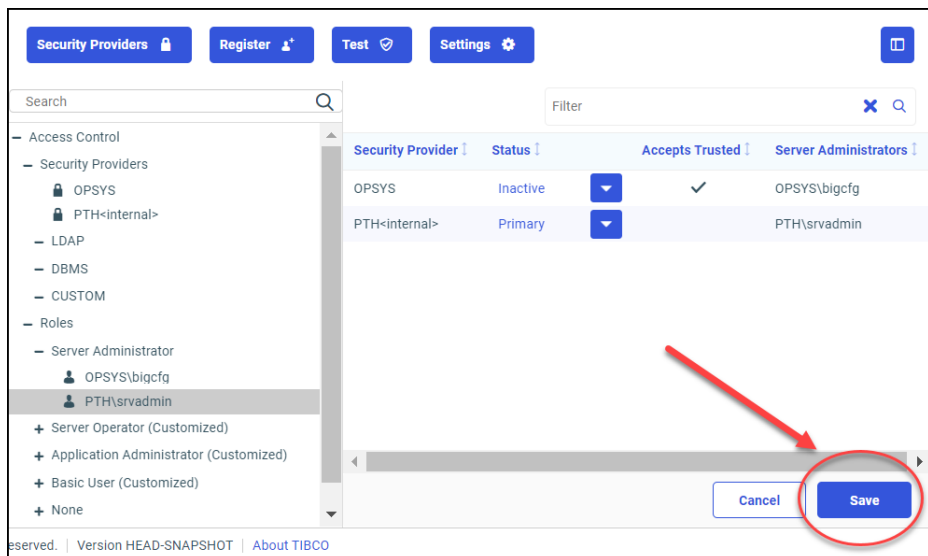
1. Open the Access Control page of the Reporting Server browser interface. If prompted, sign in with a valid Server Administrator User ID, Password, and Security Provider, if the Security Provider list appears on the Sign in page.

2. Identify the entry for the new primary security provider, select *Primary* in the Status list, as shown in the following image.



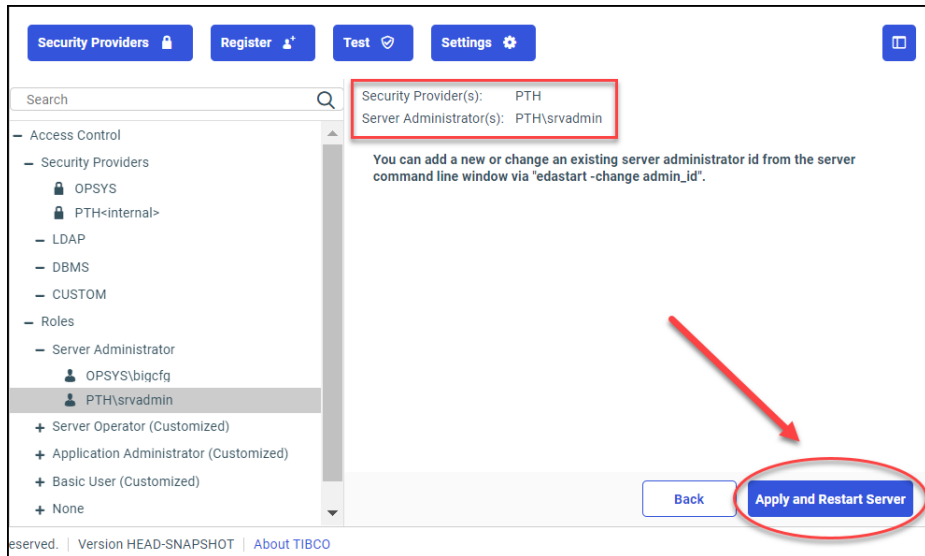
If you previously selected a Primary security provider, the status of that provider automatically changes to Secondary.

3. Review your revised configuration, and select *Save*, as shown in the following image.





4. Review the confirmation page, and select *Apply and Restart Server*, as shown in the following image.

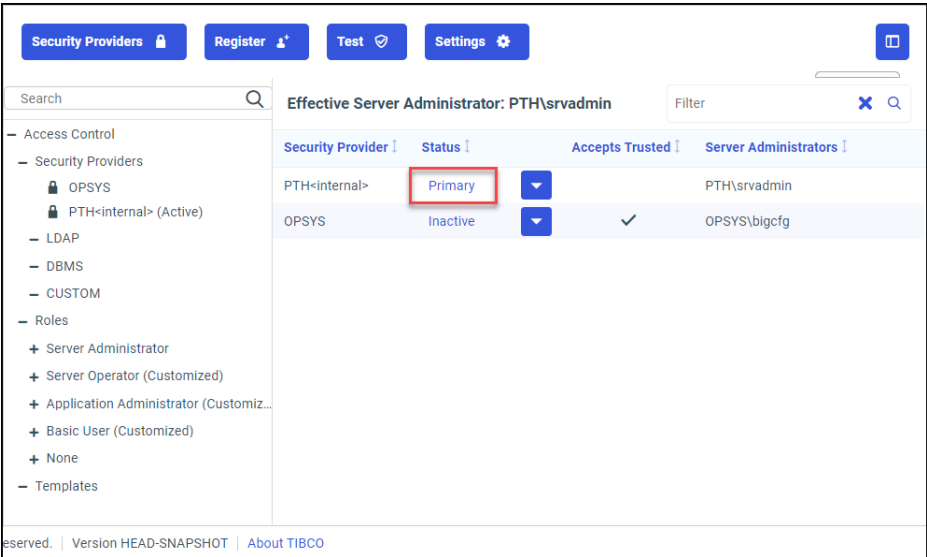


The WebFOCUS Reporting Server displays a message notifying you that it is restarting.

**Note:**

- ☐ The WebFOCUS Reporting Server must always be restarted manually when you make OPSYS the primary provider.
  - ☐ If the browser displays the *Workspace restarting* message for more than 30 seconds, close and re-open the browser. You should now be able to sign in to the Reporting Server browser interface.
  - ☐ If the new primary provider did not identify a Server Administrator, the WebFOCUS Reporting Server notifies you that it is adding a new provider and asks you to register a Server Administrator for the provider. You can register the new Server Administrator as described in [How to Register a User Account as a Server Administrator](#) on page 41.
5. After the WebFOCUS Reporting Server restarts, sign in with the user ID and password of the Server Administrator of the new primary security provider. The Applications page opens in response.
  6. Perform one of the following steps to navigate to the Access Control page.
    - ☐ If you are on the Hub, refresh the browser to redisplay the Access Control Page.
    - ☐ If you are in the Reporting Server browser interface, select *Tools* and *Access Control* to return to the Access Control page.

7. In the list of Security Providers on the Access Control page, confirm that the new status appears next to the Security Provider name, as shown in the following image.



**Procedure:** How to Change the Status of a Security Provider

**Before you begin:** Ensure that you have created a security administrator for the new primary security provider as described in [How to Register a User Account as a Server Administrator](#) on page 41. You will be unable to access the Reporting Server browser interface after designating a new primary security provider if you do not have an administrator for it.

Only one Security Provider can be identified as the Primary Security Provider within the WebFOCUS Reporting Server configuration. Therefore, when you replace an existing primary security provider with a different security provider, the existing primary security provider automatically becomes a secondary security provider.

When changing security providers, we recommend that you always retain PTH<internal> as a secondary security provider. This practice ensures that you can continue to access the WebFOCUS Reporting Server, even if the primary security provider becomes unavailable.

1. Navigate to the Access Control page of the Reporting Server browser interface. If prompted, sign in with a valid Server Administrator User ID, Password. and select a Security Provider, if the Security Provider list appears on the Sign in page.
2. For each security provider you want to change, perform one of the following steps:
  - a. Select *Primary* to activate the provider as the primary security provider.

**Note:** If another security provider is already identified as the primary security provider, the status of that security provider automatically changes to Secondary.

- b. Select *Secondary* to activate the provider as an alternative security provider.
- c. Select *Inactive* to deactivate the provider.

The tab refreshes after each selection.

- 3. When the tab refreshes, click **Save**.
- 4. Review the confirmation message prompting you to confirm that the designated security administrator ID is valid within your newly chosen Primary Security provider, and select *Apply and Restart Server*.

**Note:** If you have activated the OPSYS security provider but have not yet identified a Server Administrator for OPSYS, you receive a message prompting you to register a Server Administrator for the OPSYS security provider, follow the steps described in [How to Register a User Account as a Server Administrator](#) on page 41.

If you do not receive this message, continue with the following step.

The WebFOCUS Reporting Server displays a message notifying you that it is restarting.

- 5. When you receive a message that the WebFOCUS Reporting Server is restarting, wait until the WebFOCUS Reporting Server has started again.

**Notes:**

- ☐ The WebFOCUS Reporting Server must always be restarted manually when you make OPSYS the primary provider.
- ☐ If the browser displays the *Workspace restarting* message for more than 30 seconds, close and re-open the browser. You should now be able to sign in to the Reporting Server browser interface.
- 6. If prompted, sign in to the WebFOCUS Reporting Server again with a valid Server Administrator User ID, Password, and Security Provider.
- 7. On the Home Page of the Reporting Server browser interface, select *Tools* and *Access Control* to open the Access Control page.
- 8. In the list of Security Providers on the Access Control page, confirm that the new status appears next to the updated Security Provider names.

**Reference: Security Provider Calls**

The following table lists the requests that are used to retrieve security information from the WebFOCUS Reporting Server.

<b>WebFOCUS Request (shown in event.log)</b>	<b>Corresponding Server Message</b>	<b>Definition</b>
getProviders()	get all providers	Retrieves the security providers configured on the WebFOCUS Reporting Server node that is used for external authentication or authorization.
authConnect	authenticate and get user info, <i>u=userid</i>	When your installation is configured to use external authentication, authenticates users and retrieves user descriptions and email addresses from the security provider.
getGroupsForUser()	get groups, <i>u=userid</i>	Retrieves external group memberships or other external authorization information for a user. Also generates group membership reports for users in the Security Center.
getUsersForGroup()	get users, <i>g=group</i>	Retrieves the users who belong to a mapped group.
getGroups() [mask:searchstring]	get groups, [ <i>g=searchstring,</i> <i>provider=providerName</i>	Retrieves external groups or other attributes used for external authorization when you click the <i>Browse</i> button in the Edit Group dialog box.
getUsers()	get user info, <i>u=userid,</i> <i>provider=providerName</i>	Retrieves the user description and email in pre-authenticated configurations.

## Configuring Trusted Connections

You can configure a trusted connection between the WebFOCUS Client and the WebFOCUS Reporting Server and between the ReportCaster Distribution Server and the WebFOCUS Reporting Server.

A trusted connection is the recommended approach and has multiple benefits:

- ☐ For external authentication, a trusted connection efficiently connects to the WebFOCUS Reporting Server, and does not require additional authentication requests against the Authentication provider, which can decrease system performance.
- ☐ For pre-authentication, a trusted connection prevents the WebFOCUS Reporting Server from prompting the user for credentials.

**Note:** You must enable the WebFOCUS Reporting Server to accept trusted connections. For more information, see [How to Configure the TIBCO WebFOCUS Reporting Server to Accept Trusted Connections](#) on page 51.

### **Procedure:** How to Configure the WebFOCUS Client to Make a Trusted Connection to the TIBCO WebFOCUS Reporting Server

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, expand the *Reporting Servers* folder, and then expand the *Server Connections* folder.

The list of existing WebFOCUS Reporting Server Connections appears in the tree.

3. Click the node of the WebFOCUS Reporting Server for which you must establish a trusted connection.

The Client Configuration page opens.

4. In the Security field, click *Trusted*. A trusted connection passes the WebFOCUS user ID to the WebFOCUS Reporting Server.
5. You can choose to include or omit user group information.
  - a. To include user group information, click *Pass TIBCO WebFOCUS User ID and their Groups*. This is the default. Proceed to step 7.
  - b. To omit user group information, click *Custom*. Continue with step 6.
6. The User ID and User's Groups check boxes and associated options appear.
  - a. The User ID check box is automatically selected because user IDs must be passed to the WebFOCUS Reporting Server.

- ☐ Do not change the TIBCO WebFOCUS script variable. It must be *IBIMR\_user*.

- ☐ Click HTTP Header Field if you wish to pass user IDs with this method instead of the script variable. Type the HTTP Header Field file name.
  - b. Clear the User's Groups check box to prevent group information from being passed to the WebFOCUS Reporting Server. Leave the check box selected to pass user group information to the WebFOCUS Reporting Server.
  - ☐ Use the default WebFOCUS script variable *IBIMR\_memberof* or type a different variable.
  - ☐ Select HTTP Header Field if you wish to pass user group information with this method instead of the script variable. Type the HTTP Header Field file name.
7. Click Save.

If you have ReportCaster, you may also want to configure the ReportCaster Distribution Server to make trusted connections to the WebFOCUS Reporting Server. Otherwise, you can proceed by configuring your specific type of pre-authentication or external authentication.

**Procedure:** **How to Configure the ReportCaster Distribution Server to Make a Trusted Connection to the TIBCO WebFOCUS Reporting Server**

If you use ReportCaster, you can configure the ReportCaster Distribution Server to make trusted connections to the WebFOCUS Reporting Server when running scheduled jobs.

**Note:** Currently, trusted connections from ReportCaster in WebFOCUS send the user IDs of the schedule owners to the WebFOCUS Reporting Server, but do not send WebFOCUS groups.

1. Sign in to WebFOCUS as an administrator, and open the ReportCaster Console.
2. In the Show group, click *Configuration*.
3. Expand the *Data Servers* folder and click the folder for the desired WebFOCUS Reporting Server.
4. Select *Trusted* from the Security Type list.
5. In the *Manage Configuration* group, click Save.
6. When you receive a message asking you to confirm your decision to make changes to the ReportCaster configuration, click *OK*.
7. When you receive a message reminding you to restart the Distribution Server and reload the ReportCaster Web Application to effect these changes, click *OK*.
8. On the Reporting Server browser interface ribbon, in the *Manage Configuration* group, click *Restart*.

### **Procedure: How to Configure the TIBCO WebFOCUS Reporting Server to Accept Trusted Connections**

You can configure a security provider on the WebFOCUS Reporting Server to accept trusted connections. Each provider is configured separately. You can enable trusted connections for one provider and disable it for others.

**Note:** Trusted connections are not supported for the Windows Server OPSYS provider.

1. Open the Access Control page of the Reporting Server browser interface. If prompted, sign in with a valid Server Administrator User ID, Password, and select a Security Provider, if the Security Provider list appears on the Sign in page.
2. In the Access Control navigation pane, under Security Providers, right-click a security provider and then click *Properties*.

The Security Configuration page for that provider appears.

3. In the navigation pane, under the Security Providers folder, double-click a security provider.
4. Click *y* in the `trust_ext` list, and then click *Save*.

When you receive a message that the WebFOCUS Reporting Server is restarting, wait.

5. If the WebFOCUS Reporting Server Sign in page opens, type the Reporting Server Administrator User ID and Password and select a Security Provider, if the Security provider list appears, and then click *Sign In*.
6. When the Reporting Server browser interface home page opens, select *Tools* and *Access Control*.

A checkmark now appears in the *Accepts Trusted* column for the security provider.

## **Configuring TIBCO WebFOCUS for SSL**

The Hypertext Transfer Protocol over Secure Socket Layer (https) establishes an encrypted Secure Socket connection, and should be used to secure communications between WebFOCUS and browsers assigned to end users. There are many configuration options that enable the use of this protocol, one of which is the Apache Tomcat configuration, as described in this section.

To activate Secure Socket Layer-based communications, create a self-signed certificate for Java. You can optionally submit it to a Certificate Authority to establish it as a trusted certificate. The `keytool` utility that creates the certificate also modifies the connection type from open to SSL. Therefore, you must comment out the default Connector Protocol setting in the Tomcat `server.xml` file, and ensure that a setting for the new SSL Connector Protocol appears there instead.

Finally, the establishment of SSL security requires the replacement of the default connections between WebFOCUS and the internal applications that create graphs or deliver output to Excel spreadsheets with connections to the JSCOM3 Java-based listener. To implement this change, you must assign the value Reporting Server JCOM to the Excel Server URL (EXCELSERVURL) and Graph Server URL (GRAPHSESVURL) settings within the WebFOCUS client.

**Note:** Administrators can configure IIS to use SSL outside of their WebFOCUS configuration. For more information, see documentation provided by IIS, Tomcat, or your application server provider.

### **Procedure:** How to Create a Self-Signed Certificate

To create a Self-Signed Certificate with Java:

1. Open the command prompt window and redirect the command prompt to the *drive:\ibi\WebFOCUS82\jre\bin* directory.
2. Type the keytool command and values as shown in the following example.

```
keytool -genkeypair -alias mykey -ext san=dns:dnsName1,dns:dnsName2...  
-keyalg RSA -validity 720 -keystore /path_to_keystore/keystore  
-keysize 2048 -storepass MyPassword
```

where:

*dnsName*

Is the name, or alias, of the entity (the subject) that will present this certificate for authentication. You can include multiple names to ensure that all versions of the subject names are recognized. For multiple alternative names, use the syntax, *dns:first\_dnsName,dns:second\_dnsName,...*

For example, *dns:wfsvr,dns:wfsvr.lbi.com*.

*MyPassword*

Is the password for this keystore. You can accept MyPassword, the default value, or you can replace it with a unique password by typing it in this field.

*/path\_to\_keystore/keystore*

Is the location information that specifies where the key file will be placed. This value is optional. If you do not specify a location for the key file, the Keytool utility places it in the default location.

**Note:** The name mykey is important if you need to issue a -certreq (certificate request) for a certificate signed by a Certificate Authority.

3. Press the Enter key.

The command prompt displays the first in a series of questions.



4. Respond to each question as follows, and press Enter after each response:
  - ☐ “What is your first and last name?” Type the first and last name of the certificate holder.
  - ☐ “What is the name of your organizational unit?” Type the name of the organizational unit of the certificate holder.
  - ☐ “What is the name of your organization?” Type the name of the organization of the certificate holder.
  - ☐ “What is the name of your City or Locality?” Type the name of the city or locality of the certificate holder.
  - ☐ “What is the name of your State or Province?” Type the two-letter abbreviation for the state in which the certificate holder is located.
  - ☐ “What is the two-letter country code for this unit?” Type the two-letter abbreviation for the country in which the certificate holder is located.
5. When the command prompt displays the question, “Is CN=\_\_, OU=\_\_, O=\_\_, L=\_\_, ST=\_\_, C=\_\_ correct?”, review the values and type *y* if they are correct.
 

If they are not correct, Type *n* and retype the keytool command from step 2.

If they are correct, the new Self-Signed Certificate is ready for use.

**Reference: Establishing the Self-Signed Certificate as a Trusted Certificate**

Until you identify the new self-signed certificate to the browser as a Trusted Certificate, the browser will display errors when you use it. During the initial testing period, you can add the new self-signed certificate directly to the Trusted Certificate Authority of those browsers included in the test. However, to fully establish the new certificate as a trusted certificate, you typically request certification for it from a Certificate Authority using the following request:

```
keytool -certreq -alias mykey -storepass MyPassword -file ./mykey.csr
-keystore /path_to_keystore/keystore
```

where:

*MyPassword*

Is the password for this keystore. You can accept MyPassword, the default value, or you can replace it with a unique password by typing it in this field.

*/path\_to\_keystore/keystore*

Is the location information that specifies where the key file will be placed. This value is optional. If you do not specify a location for the key file, the Keytool utility places it in the default location.

You can then send the certificate request file (mykey.csr) to a Certificate Authority to sign, and when the authority returns the signed certificate, import it into the keystore.

### **Reference: Importing the Trusted Certificate into the Keystore**

To import your certificate from an external Certificate Authority (CA), type the following command:

```
keytool -import -alias mykey -file ./mykey.crt -keystore /path_to_keystore/keystore
```

where:

*/path\_to\_keystore/keystore*

Is the location information that specifies where the key file will be placed. This value is optional. If you do not specify a location for the key file, the Keytool utility places it in the default location.

If your CA is an internal CA, then type the following command to import the certificate from your Certificate Authority.

```
keytool -import -alias CA -trustcacerts -file ./ca.crt -keystore /path_to_keystore/keystore
```

where:

*/path\_to\_keystore/keystore*

Is the location information that specifies where the key file will be placed. This value is optional. If you do not specify a location for the key file, the Keytool utility places it in the default location.

**Reference: Updating the Connector Protocols in the Tomcat Server.xml File**

If you included Tomcat in your product installation, the server.xml file for Tomcat is located in the following directory:

`C:\ibi\tomcat\conf`

The keytool utility disables the http connection assigned to port 26000. Therefore you must comment out the Connector tag in the server.xml file that defines this http-based connection by typing an exclamation point (!) after the open tag symbol (<).

```
<Connector connectionTimeout="20000" maxPostSize="-1" port="26000"
protocol="HTTP/1.1" redirectPort="26001" useBodyEncodingForURI="true"/>
```

The keytool utility also establishes an SSL connector on port 443. This connection replaces the old http based connection. Therefore, if it does not appear in the file, you must type this updated version of the connector tag, with its attributes and values, as shown in the following example:

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
port="443" SSLEnabled="true"
keystoreFile="C:/users/path_to_keystore/keystore"
keystorePass="MyPassword"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA"/>
```

where:

`/path_to_keystore/keystore`

Is the location information that specifies where the key file will be placed. This value is optional. If you do not specify a location for the key file, the Keytool utility places it in the default location.

`MyPassword`

Is the password for this keystore. You can accept MyPassword, the default value, or you can replace it with a unique password by typing it in this field.

**Procedure: How to Change the TIBCO WebFOCUS Configuration to Support SSL**

Before you begin, ensure the JSCOM service is configured and operational on the WebFOCUS Reporting Server. For more information, see *How to Configure Java Services for a JSCOM3 Listener* in the *TIBCO WebFOCUS® Reporting Server Administration Manual*.

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, under Application Settings, click *Client Settings*.

3. Click *Reporting Server JSCOM* in the Excel Server URL list.
4. Click *Reporting Server JSCOM* in the Graph Server URL list.
5. Click *Save*.
6. When you receive the *Successfully Saved* message, click *OK*.

## TIBCO WebFOCUS Reporting Server Profiles

The following profiles can be used to configure default behavior on the WebFOCUS Reporting Server:

- ❑ **WebFOCUS Reporting Server global profile (edasprof.prf).** The global profile is a startup file that is automatically created during Server installation. It contains the default environmental settings for the Reporting Server. The global profile remains in effect throughout a user session.
- ❑ **WebFOCUS Reporting Server service profile.** A service profile is a file used by the Reporting Server to specify environmental settings for connections associated with a specific service. When the Client connects to the Server with a service qualifier, the service profile settings are applied and remain in effect throughout the user session. A service profile may contain settings that are the same as those in a global profile.
- ❑ **WebFOCUS Reporting Server group profiles.** A group profile is a file used by the Reporting Server to specify environmental settings for users in a specific security group. Upon connection to the server by a user, the group profile settings are applied. They remain in effect throughout the Reporting Server session. Group profiles may contain settings that are for the most part defined by the same set of commands as those used in a global profile. This profile is only available if security is ON. For more information about group profile processing, see the *Server Administration* manual for your operating system.
- ❑ **WebFOCUS Reporting Server individual user profiles (userid.prf).** A user profile is a file used by the Reporting Server to specify environmental settings for a specific user ID. When the user connects to the Reporting Server, the user profile settings are applied. They remain in effect throughout the user session. User profiles may contain settings that are for the most part defined by the same set of commands used in a global profile.

For more information, see the *Server Administration* manual for your operating system.

## Sending Variables to the TIBCO WebFOCUS Reporting Server Profile

Secure requests sent from the Client to the Reporting Server can include a list of variables and their associated values that enable the Reporting Server profile, using conditional logic, to activate different DBMS settings and create a customized server environment. For example, one set of values could activate a test environment and a different set of values could activate a production environment.

For Managed Reporting Requests, these variables, their associated values, and DBMS connection information, can be defined in the Managed Reporting Workspace from which the request originated. For APP requests, they can be defined in the HTTP Host Header from which the request originated. The variables and their associated values must be established on a Client, and the values assigned to variables by that client must not be overridden when included in a URL. A Client can deliver a unique set of variables and their associated values to an individual server or to all servers.

To configure support for the use of variables in client requests, an Administrator must type a list of variables in the Custom Settings list to include in requests submitted by that client to the Reporting Server, identify the variables to send to all Reporting Servers, identify those to send to individual Reporting Servers, and identify the database containing those variables in the Reporting Server profile.

### **Procedure:** How to Configure Variables to Include in TIBCO WebFOCUS Reporting Server Requests

Only an administrator can configure a list of variables and their associated values for a client.

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, click *Custom Settings*.
3. To define the list of variables and the values assigned to them to send from this client:
  - a. In the Custom Settings list, type the comment line:

`#variables and values`

- b. Type an entry for each variable and value using the following format:

`VariableName=Value`

Where:

`VariableName`

Is the name of a variable that you want to send from this client. This variable must appear in the database of variables connected to the Reporting Servers that will receive these requests.

*Value*

Is the specific value for the variable that you want to send from this client.

For example:

```
#variables and values
```

```
IBI_pvar=XPROFILE
```

```
IBI_clientName=Client1
```

```
ABCVar=Test2
```

4. To define a list of variables to send to all servers:

- a. In the Custom Settings list, type the comment line:

```
#List of profile variables to be sent to all eda servers
```

- b. Then type the command:

```
IBIC_profileVars=Variable1;Variable2;...
```

Where:

*Variable#*

Is a variable defined in the list of variables and values.

For example:

```
#List of profile variables to be sent to all eda servers
```

```
IBIC_profileVars=IBI_pvar;IBI_clientName;
```

5. To define a list of variables to send to a specific server:

- a. In the Custom Settings list, type the comment line:

```
#list of profile variables to be sent ONLY to server named ServerName
```

Where:

*ServerName*

Is the name of the specific server to which the list of variables must be sent.

- b. Then type the command:

```
IBIC_profileVars_ServerName=Variable1;Variable2;
```

Where:

*ServerName*

Is the name of the specific server to which the list of variables must be sent.

*Variable#*

Is a variable defined in the list of variables and values.

For example:

```
#list of profile variables to be sent ONLY to server named EDASERVE
IBIC_profileVars_EDASERVE=ABCVar;
```

6. Click Save.
7. When you receive the Successfully Saved message, click OK.

**Procedure: How to Adapt the TIBCO WebFOCUS Reporting Server Profile to Accept Variables in Client Requests**

The administrator must also update the server profile by adding the following statement to the end of the Server Profile list.

1. In the Administration Console, on the Configuration tab, expand the Reporting Servers folder.
2. Under the Server Connections folder, right-click EDASERVE, and then click *Profile*.
3. In the EDASERVE.prf list, type:

```
APP FILEDEF &IBI_pvar bugs/DatabaseName.dat
```

Where:

*DatabaseName*

Is the name of the database linked to the Reporting Server.

For example:

```
APP FILEDEF &IBI_pvar bugs/edasprof.dat
```

4. Click Save.
5. When you receive the Successfully Saved message, click OK.





## Configuring the TIBCO WebFOCUS Client

---

You can configure and manage the WebFOCUS Client using the Administration Console. The Administration Console enables you to update WebFOCUS configuration settings, enable logs and traces, monitor WebFOCUS sessions, and verify WebFOCUS components. You can also edit configuration files manually.

### In this chapter:

- ❑ [TIBCO WebFOCUS Configuration Files](#)
  - ❑ [Using the TIBCO WebFOCUS Administration Console](#)
  - ❑ [Configuring and Customizing Your Environment](#)
  - ❑ [Configuring TIBCO WebFOCUS Security](#)
  - ❑ [Working With TIBCO WebFOCUS Diagnostics](#)
  - ❑ [DBA Password Settings](#)
  - ❑ [Stopping a Report Request](#)
- 

### TIBCO WebFOCUS Configuration Files

WebFOCUS configuration files are located in the *drive:\ibi\WebFOCUS82\config* folder. These files can be moved easily from one environment to another to transfer configuration settings.

During installation, WebFOCUS writes the default configuration values that you choose to a bootstrap file (*web.xml*) and to the installation configuration file (*install.cfg*). When you modify the configuration behavior for most settings, the new values are written to the *webfocus.cfg* file. When WebFOCUS starts, first it checks the bootstrap file for the *IBI\_DOCUMENT\_ROOT* setting, which tells WebFOCUS where to look for many directories. Using the *IBI\_DOCUMENT\_ROOT* value, WebFOCUS then looks for the product defaults specified by Java code, then checks the installation defaults specified by *install.cfg*, and then the checks the modifications specified by *webfocus.cfg*. All of these actions are recorded in the *event.log*.

For more information about the *event.log*, see [Logging](#) on page 591.

WebFOCUS automatically encrypts any password that you enter directly into a configuration file, such as `install.cfg` or `webfocus.cfg`, the next time that you start the application or run a command line utility, such as Change Management. There is no need to run a separate encryption utility.

Security configuration settings that are written into files other than `webfocus.cfg` include security zone configuration files, such as `securitysettings.xml`. For more information, see [TIBCO WebFOCUS Client Configuration Files](#) on page 511.

When placed at the start of a line in a configuration file, the number sign (#) character converts the text on that line into a comment, excluding the variables or commands in that line from execution when WebFOCUS invokes this file. You can use this feature to convert a variable into a comment. You can also use this feature to add comments that include notes, explanations, and reminders about settings and the values assigned to them that appear in these files.

To convert a variable to a comment, type a number sign (#) as the first character of the line in which the variable appears. To add a comment, start a new line, type the number sign (#), and then type a brief note, explanation, or reminder. When your changes are complete, click *Clear Cache* from the Administration Console menu bar to save the changes to your configuration file.

## Using the TIBCO WebFOCUS Administration Console

The WebFOCUS Administration Console contains the settings that configure the WebFOCUS Client, customize internal or external authentication settings, connect you to ReportCaster, and support diagnostic research.

### Opening the TIBCO WebFOCUS Administration Console

Because the Administration Console contains settings that can alter the operation of your entire WebFOCUS installation, it is available only to those users with the privileges to update or reconfigure system settings.

Therefore, before you can open the Administration Console, you must sign in with a User ID that is assigned to the Administrators Group and therefore automatically includes the *Display Administration Console* (`opWFAdminConsole`) Session privilege in the Administrator Privilege Category and the *Access Resource* (`opList`) all subsystems privilege in the Basic Reporting category.

The *Display Administration Console* privilege gives the administrator access to the Administration Console itself. The *Access Resource* privilege gives the administrator access to the Configuration subsystem from which the settings and values displayed in the Administration Console are taken.

**Note:** As a best practice we recommend that you limit access to the Administration Console to users assigned to the Administrators group. We do not recommend that you attempt to provide access to users assigned to other groups by adding the Display Administration Console and Access Resource privileges to their user or group profile.

If your User ID includes these privileges, you can open the Administration Console by using one of the following methods.

On the Hub:

- ❑ In the side navigation pane, select *Management Center* and then, under *Client Administration*, select *Administration Console*.

On the WebFOCUS Home Page:

- ❑ Click your *User Account Icon*, point to *Administration*, and then click *Administration Console*.

In the browser address bar:

- ❑ Type the following URL:

`http(s)://host:port/context/admin`

where:

*host*

Is the name or IP address of the host used to access WebFOCUS.

*port*

Is the number of the port on which the Web Server or Application Server listens.

This value is optional, and it should be excluded if the URL uses the default port for the protocol it uses in the scheme, which is port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

*context*

Is the specific context used for WebFOCUS. For example, *ibi\_apps*.

**Note:** If you are signed into WebFOCUS, and the machine id, port, and context already appear in the address bar, you only need to type over that part of the path that follows the context with the term */admin*.

**Procedure: How to Sign In to the Administration Console From the Start Menu**

1. If WebFOCUS has been installed on a Windows 7 machine:
  - a. Click the *Start* button, and then expand the *Information Builders* folder.
  - b. Expand the *WebFOCUS 82* folder, and then click *WebFOCUS Administration Console*.
  - c. Continue with step 3.
2. If WebFOCUS has been installed on a Windows 10 machine:
  - a. Click the *Start* button.
  - b. Scroll down the Apps list to the *Information Builders* folder.
  - c. If you are using the Integrated Installation of WebFOCUS, select the *Windows Integrated Installation* folder to open the Windows Integrated Installation File Explorer window, and select *Run WebFOCUS*, and sign in.

Perform one of the following steps to open the Administration Console.

- ☐ On the Hub, in the side navigation pane, select *Management Center*, and then, under *Client Administration*, select *Administration Console*.

Or

- ☐ From the User Menu, select *Switch Homepage*, and *WebFOCUS Homepage*. In the banner of the WebFOCUS Home page, select *Settings*, and then select *Administration Console*.
- d. If you are not using the Integrated Installation of WebFOCUS, expand the *Information Builders* folder, select *WebFOCUS Administration Console*, and sign in with the User Name and Password of a user who has privileges to open the Administration Console.

**Procedure: How to Sign in to the Administration Console From a Browser Window**

1. Go to the URL:  
`http(s)://host:port/context/admin`

where:

`host`

Is the name or IP address of the host used to access WebFOCUS.

`port`

Is the number of the port on which the Web Server or Application Server listens.

This value is optional, and it should be excluded if the URL uses the default port for the protocol it uses in the scheme, which is port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

*context*

Is the specific context used for WebFOCUS. For example, *ibi\_apps*.

2. On the Sign in page, type the *User Name* and *Password* of a user that has privileges to open the Administration Console, and click *Sign in*.

The Administration Console opens automatically.

**Note:** To display the Administration Console using a different language, on the Sign in page click Chose language and then click the language you want to use in the language list.

## Opening the ReportCaster Console

You can make global configuration changes in the ReportCaster server environment by using the ReportCaster Console. WebFOCUS makes the ReportCaster Console available to you from the Main Menu on the Hub, from the Utilities menu on the WebFOCUS Home Page, and from the ReportCaster tab on the Administration Console.

Before you can open the ReportCaster Console, you must sign in with a User ID that has the privilege to do so. You can then open the ReportCaster Console by selecting one of the following methods.

On the Hub:

- ☐ Above the side navigation pane, select *Main Menu*, and under *Quick Access*, select *ReportCaster Status*.

On the WebFOCUS Home Page:

- ☐ In the banner, select *Utilities*, and then select *ReportCaster Status*.

or

- ☐ In the banner, select *Utilities*, and then select *Administration Console*. On the Administration Console, click the *ReportCaster* tab.

For more information about ReportCaster, see the *TIBCO WebFOCUS® ReportCaster Guide*.

## Working With Home Pages

The Redirect */ibi\_apps* to setting defines the default landing page for your product installation.

Once you have started your work session, you can open any of these home pages, regardless of your default home page configuration. This capability is especially important if you need to use features that are only available on that page.

You can also sign in to any home page by typing the URL for it in your browser window. However, you will return to the default home page defined in the Redirect `/ibi_apps` to setting during your work session.

**Note:** The name assigned to the Redirect `/ibi_apps` to setting can vary, depending upon the name assigned to the main context or alias in use in your configuration of WebFOCUS. This setting typically displays the term `/ibi_apps` because that term is typically used as the main context or alias for an installation of WebFOCUS. If your organization uses a different main context or alias, that value will appear in this setting instead. Regardless of the main context name assigned to it, this setting appears as the first setting on the BI Portal settings page of the Configuration tab in the Administration Console.

### **Procedure:** How to Open the Hub From a Browser Window

You can open the Hub by typing the basic context URL your browser.

1. In the browser address bar, type the following URL:

`http(s)://host:port/context/`

where:

`host`

Is the name or IP address of the host used to access TIBCO WebFOCUS.

`port`

Is the number of the port on which the Web Server or Application Server listens.

This value is optional, and it should be excluded if the URL uses the default port for the protocol it uses in the scheme, which is port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

`context`

Is the specific context used for TIBCO WebFOCUS. For example, `ibi_apps`.

**Note:** If you are signed in, and the machine id, port, and context already appear in the address bar, you only need to clear that part of the path that follows the context.

2. If your user authentication method does not require you to sign in, or if you are already authenticated, the Hub opens automatically.
3. If your user authentication method requires you to sign in, on the Sign in page, type a valid User name and Password, and then click *Sign in*.

The Hub opens in response.

### **Procedure:** How to Open the WebFOCUS Home Page From a Browser Window

You can open the WebFOCUS Home Page by typing the URL for it in your browser.

1. In the browser address bar, type the following URL:

`http(s)://host:port/context/home`

where:

`host`

Is the name or IP address of the host used to access WebFOCUS.

`port`

Is the number of the port on which the Web Server or Application Server listens.

This value is optional, and it should be excluded if the URL uses the default port for the protocol it uses in the scheme, which is port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

`context`

Is the specific context used for WebFOCUS. For example, *ibi\_apps*.

**Note:** If you are signed in, and the machine ID, port, and context already appear in the address bar, you only need to type over that part of the path that follows the context with the term */home*.

`home`

Is the case-sensitive path that opens the WebFOCUS Home Page.

2. If your user authentication method does not require you to sign in, or if you are already authenticated, the WebFOCUS Home Page opens automatically.
3. If your user authentication method requires you to sign in, on the Sign in page, type a valid User name and Password, and then click *Sign in*.

The WebFOCUS Home Page opens in response.

### **Procedure:** How to Open the Legacy Home Page From a Browser Window

You can open the Legacy Home Page by typing the URL for it in your browser.

1. In the browser address bar, type the following URL:

`http(s)://host:port/context/legacyhome`

where:

*host*

Is the name or IP address of the host used to access WebFOCUS.

*port*

Is the number of the port on which the Web Server or Application Server listens.

This value is optional, and it should be excluded if the URL uses the default port for the protocol it uses in the scheme, which is port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

*context*

Is the specific context used for WebFOCUS. For example, *ibi\_apps*.

*legacyhome*

Is the case-sensitive path that opens the Legacy Home Page.

For example:

[https://Server01:8080/ibi\\_apps/legacyhome](https://Server01:8080/ibi_apps/legacyhome)

2. If your user authentication method does not require you to sign in, or if you are already authenticated, the Legacy Home Page opens automatically.
3. If your user authentication method requires you to sign in, on the Sign in page, type a valid User name and Password, and then click *Sign in*.

The Legacy Home Page opens in response.

### ***Procedure:*** How to Switch Home Pages

The Switch Home Page option on the User menu allows you to open and work with a different Home Page.

On the Hub, expand the *User* menu, select the *Switch Home Page* option, and then select either *WebFOCUS Home Page* or *Legacy Home Page*.

### ***Procedure:*** How to Open the Legacy Home Page From the WebFOCUS Home Page

On the WebFOCUS Home Page, in the User menu, click *Legacy Home Page*.

**Note:** If the *Show Legacy Home Page option in Banner Links* check box is cleared in the *Redirect /ibi\_apps* to setting, located on the BI Portal pane of the Administration Console Configuration Tab, the *Legacy Home Page* command will not be visible.



**Procedure: How to Open a Custom Welcome Page From a Browser Window**

You can open a Custom Welcome Page by typing the URL for it in your browser.

1. In the browser address bar, type the following URL:

`http(s)://host:port/context/path`

where:

`host`

Is the name or IP address of the host used to access WebFOCUS.

`port`

Is the number of the port on which the Web Server or Application Server listens.

This value is optional, and it should be excluded if the URL uses the default port for the protocol it uses in the scheme, which is port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

`context`

Is the specific context used for WebFOCUS. For example, *ibi\_apps*.

`path`

Is the case-sensitive path that opens the Custom Welcome Page.

**Note:** If you are signed in, and the machine id, port, and context already appear in the address bar, you only need to type over that part of the path that appears after the context with the remaining path to the Custom Welcome Page.

2. If your user authentication method does not require you to sign in, or if you are already authenticated, the Custom Welcome Page opens automatically.
3. If your user authentication method requires you to sign in, on the Sign in page, type a valid User name and Password, and then click *Sign in*.

The Custom Welcome Page opens in response.

**Navigating the TIBCO WebFOCUS Administration Console**

The Administration Console contains a menu bar and four tabs that help you navigate to its settings and other features.

These tabs organize administration activities into the following categories:

- ❑ **Configuration.** Configures Reporting Server connections, Application Settings, Custom Settings, NLS Settings, Redirection Settings, the Dynamic Language Switch, and InfoAssist Properties. This tab also connects you to the Role Update Utility and HTML5 Chart Extensions.
- ❑ **Security.** Configures general security settings for Internal and External Authentication, and zone-based settings for Authentication, and Request Matching.
- ❑ **ReportCaster.** Opens the ReportCaster Console where you can configure ReportCaster, restart the Distribution Server, configure environment parameters, and turn traces on and off. The Administration Console authenticates to ReportCaster with the value of the user ID, IBIMR\_RC\_SVCUSER. If this authentication fails, users are prompted for their credentials.
- ❑ **Diagnostics.** Displays component installation and configuration details, turns WebFOCUS logging on or off, and enables administrators to view or create zip copies of log files. This tab also connects you application file logs, created when you run stand-alone utilities, and to the Lru Cache statistics page.

You can view traces with the Session Viewer, which is accessible from one of the following locations.

- ❑ From the Hub, select the *View Sessions* option from the *Tools* menu.
- ❑ From the WebFOCUS Home Page, select the *Session Viewer* option from the *Utilities* menu.
- ❑ From the Legacy Home Page, select the *Session Viewer* option from the *Tools* menu on the BI Portal Menu bar.

Options on the menu bar connect you to such basic tasks as reviewing TIBCO WebFOCUS and third party licensing information, clearing the cache, closing the Administration Console when you open it from the WebFOCUS Home Page or the Legacy home page, or opening Help.

To update or review an Administration Console setting, click a tab, and then click the folder or page icon from the main menu on your selected tab. The main window refreshes and the individual settings assigned to your selected page become available.

## Navigating the Configuration Tab

The Configuration tab contains settings and features that describe Reporting Server connections and other application settings, which are listed and described in the following table.

Folder [Page]	Available Functionality
<b>Reporting Servers</b>	<p>The Reporting Servers subfolders contain the tools that manage all connections from the Client to individual reporting servers. Using the following sub-folders, you can:</p> <ul style="list-style-type: none"><li><input type="checkbox"/> <b>Server Connections.</b> Add and change Remote Services settings.</li><li><input type="checkbox"/> <b>Alternate Server Mappings.</b> Configure alternate mappings to individual Remote Servers.</li><li><input type="checkbox"/> <b>Cluster Mappings.</b> Configure a detailed connection from the client to multiple Remote Servers that includes security settings, encryption methods, and time-out limits.</li><li><input type="checkbox"/> <b>Legacy Cluster Configurations.</b> Configure a basic connection from the client to multiple Remote Servers that includes no additional details.</li></ul>

Folder [Page]	Available Functionality
<b>Configuration</b> <b>[Application Settings]</b>	<p>Pages in the Application Settings folder of the Configuration tab include settings for the following functional areas:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Application Caches</li> <li><input type="checkbox"/> Application Contexts</li> <li><input type="checkbox"/> Application Directories</li> <li><input type="checkbox"/> BI Portal</li> <li><input type="checkbox"/> Change Management</li> <li><input type="checkbox"/> Client Settings</li> <li><input type="checkbox"/> Deferred Reporting</li> <li><input type="checkbox"/> Diagnostic/Tracing</li> <li><input type="checkbox"/> Encryption</li> <li><input type="checkbox"/> ESRI</li> <li><input type="checkbox"/> Filters</li> <li><input type="checkbox"/> Magnify</li> <li><input type="checkbox"/> Multiple Reports</li> <li><input type="checkbox"/> On-Demand Paging</li> <li><input type="checkbox"/> OLAP*</li> <li><input type="checkbox"/> Other</li> <li><input type="checkbox"/> Parameter Prompting</li> <li><input type="checkbox"/> Quick Data</li> <li><input type="checkbox"/> Repository</li> <li><input type="checkbox"/> Source Code Management</li> <li><input type="checkbox"/> Search</li> <li><input type="checkbox"/> Text Generation Server</li> <li><input type="checkbox"/> Validation</li> </ul> <p>*OLAP settings are visible only if the Enable OLAP check box has been selected.</p>

Folder [Page]	Available Functionality
<b>Configuration</b> <b>[Custom Settings]</b>	<p>The Custom Settings page of the Configuration tab contains a text-based input field where you can define advanced customization settings for the Client. Using this page, you can:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Customize Client settings.</li> <li><input type="checkbox"/> Create a Client site profile.</li> <li><input type="checkbox"/> Create a Client universal profile.</li> <li><input type="checkbox"/> Configure custom variables to include in Reporting Server requests.</li> </ul>
<b>Configuration</b> <b>[NLS Settings]</b>	<p>The NLS Settings page of the Configuration tab contains National Language Support settings.</p>
<b>Configuration</b> <b>[Dynamic Language Switch]</b>	<p>The Dynamic Language Switch page of the Configuration tab contains a list of languages that can be included in this product installation.</p> <p>Dynamic Language Switch settings are stored in the languages.xml file located in the <i>drive:\ibi\WebFOCUS82\config</i> directory.</p>
<b>Configuration</b> <b>[Redirection Settings]</b>	<p>The Redirection Settings page of the Configuration tab contains settings that manage the redirection of report output.</p>
<b>Configuration</b> <b>[InfoAssist Properties]</b>	<p>The InfoAssist Properties page of the Configuration tab contains properties that configure reporting options in the InfoAssist reporting tool.</p>
<b>Configuration</b> <b>[Role Update Utility]</b>	<p>The Role Update Utility page of the Configuration tab contains settings that identify the differences between the privileges currently assigned to roles in the repository and their corresponding package roles.</p>

Folder [Page]	Available Functionality
<b>Configuration</b> <b>[HTML5 Chart Extensions]</b>	The HTML5 Chart Extensions page of the Configuration tab contains all HTML5 chart extensions currently installed in your local installation. Features on this page allow you to upload HTML5 chart extensions, enable or disable their use in InfoAssist and WebFOCUS Designer, and uninstall them when no longer needed.

## Navigating the Security Tab

The Security tab contains internal, external, and advanced security settings, and the settings for security zones, which are listed and described in the following table.

Folder [Page]	Available Functionality
<b>Security Configuration</b> <b>[Internal]</b>	The Internal page of the Security tab contains sign-in and password settings for authentication and authorization managed within WebFOCUS.
<b>Security Configuration</b> <b>[External]</b>	The External page of the Security tab contains settings that define the method and location of authentication and authorization activities managed by third-party applications outside of WebFOCUS.
<b>Security Configuration</b> <b>[Advanced]</b>	The Advanced page of the Security tab contains settings that identify a Root User, an Anonymous User, and a Reporting Server Anonymous User to support security management and administration activities managed by WebFOCUS.
<b>Security Zones</b> <b>Default</b> <b>[Authentication, Request Matching]</b>	The Default Security Zone pages contain settings that identify the default authentication method used for any request not processed by one of the other zones.

Folder [Page]	Available Functionality
<b>Security Zones</b> <b>Mobile</b> <b>[Authentication, Request Matching]</b>	The Mobile Security Zone pages contain settings that define the Authentication method for TIBCO WebFOCUS mobile products, including the TIBCO WebFOCUS <sup>®</sup> Mobile App.
<b>Security Zones</b> <b>Portlet</b> <b>[Authentication, Request Matching]</b>	The Portlet Security Zone pages contain settings that define the Authentication method for Open Portal Services products, including SharePoint.
<b>Security Zones</b> <b>Alternate</b> <b>[Authentication, Request Matching]</b>	The Alternate Security Zone pages contain settings that define an alternate authentication method to that used by the Default Security Zone for requests within the same installation of WebFOCUS.

## Navigating the ReportCaster Tab

When you click the ReportCaster tab, the ReportCaster Server Status page opens, by default. Features on that page identify the current status of ReportCaster Server operations. For more information, see the *ReportCaster Users Guide*.

## Navigating the Diagnostics Tab

The Diagnostics tab contains settings and features that describe system performance and activities, which are listed and described in the following table.

Folder [Page]	Available Functionality
<b>Diagnostics</b>	<p>The Diagnostics section of the Administration Console contains the following functional areas:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <b>About TIBCO WebFOCUS.</b> Displays version and release information about your installation of TIBCO WebFOCUS.</li> <li><input type="checkbox"/> <b>Client Verification.</b> Displays your directory permissions and the status of your ability to perform common operations.</li> <li><input type="checkbox"/> <b>HTTP Request Info.</b> Displays information about HTTP request headers.</li> <li><input type="checkbox"/> <b>JVM Property Info.</b> Displays information about your Java Virtual Machine environment.</li> <li><input type="checkbox"/> <b>Session Monitor.</b> Displays session monitor events and links to detailed traces.</li> <li><input type="checkbox"/> <b>Log Files.</b> Displays links to WebFOCUS log files.</li> <li><input type="checkbox"/> <b>Application Log Files.</b> Displays links to all log files generated from application utilities.</li> <li><input type="checkbox"/> <b>Lru Cache Statistics.</b> Displays current cache usage statistics.</li> </ul>

## Using the TIBCO WebFOCUS Administration Console Menu Bar

The Administration Console menu bar appears above the Administration Console tab display. The commands and features it contains are available to all of the Administration Console tabs.

### Using the Licenses Menu

The Licenses Menu links you to information about your current TIBCO WebFOCUS license, to an audit of User and Group licenses and roles, and to information about licenses for all third-party software products included in the installation. Using Licenses menu commands you can:

- ☐ View the current license number, product edition, license key expiration date, and the number of licensed users.
- ☐ Add new license numbers, if you are operating under a Legacy license.



**Note:** To review license information about third-party software packaged with the product installation, select the *License* option from the *Help* menu on the Hub.

### Reviewing Client License Information

The *TIBCO WebFOCUS Client* menu option opens the License Information dialog box. This dialog box identifies the current license key and the individual product components made available by that key. If you are operating under a Legacy license, you can also use this dialog box to replace the current license key with a new license key when your current license expires or changes.

Available Functionality	
License Information	<p>The License Information section provides the following information:</p> <ul style="list-style-type: none"><li><input type="checkbox"/> <b>Product Edition.</b> The name of the current product edition.</li><li><input type="checkbox"/> <b>License Key.</b> The license key currently in use. Contains one of the following values.<ul style="list-style-type: none"><li><input type="checkbox"/> <b>Golden_Key.</b> This is the default value, indicating you are operating under a Golden Key license.</li><li><input type="checkbox"/> <b>Legacy License Key Number.</b> The number of the internally-managed license key assigned to you when you installed the product. Displayed when operating under a Legacy license.</li></ul></li><li><input type="checkbox"/> <b>License Key Expiration Date.</b> The expiration date of the current license. Contains one of the following values.<ul style="list-style-type: none"><li><input type="checkbox"/> <b>No Expiration.</b> This value indicates that the license has no expiration date. This value appears when you are operating under a Golden Key license.</li><li><input type="checkbox"/> <b>Expiration Date.</b> The date the license key will expire. This value appears when you are operating under a Legacy license.</li></ul></li><li><input type="checkbox"/> <b>Note:</b> If you are operating under a Legacy license, a warning message for the client license key expiration date begins to appear fourteen (14) days before the actual expiration date, by default. This message displays the expiration date and the number of days remaining until that date. The License Expiration Warning message appears only to Administrators during sign in, and it is written to the event.log file located in the logs directory of the Client installation.</li></ul>

Available Functionality

- ☐ **User Licenses.** The total number of available user licenses and the number of licenses used for each user category. Contains one of the following values.
  - ☐ **Unlimited.** This value indicates that there is no limit on the maximum number of users. It appears when you are operating under a Golden Key license, and is the default value under that license.
  - ☐ **Number.** This value identifies the total number of available user licenses and the number of licenses used for each user category. It appears when you are operating under a Legacy license, and can include the following user categories:
    - ☐ Total Users
    - ☐ Portal Users
    - ☐ Designer/InfoAssist Users
- ☐ **Product Components.** The product components your license entitles you to use. If the check box to the right of an entry is visible and selected, you are entitled to use that product component.
  - ☐ TIBCO WebFOCUS Client Self Service
  - ☐ TIBCO WebFOCUS Portal
  - ☐ Designer/InfoAssist
  - ☐ InfoAssist Basic
  - ☐ TIBCO WebFOCUS Mobile
  - ☐ Magnify
  - ☐ Quick Data
  - ☐ ReportCaster
  - ☐ Web Services
  - ☐ Open Portal Services
  - ☐ Data Visualization
  - ☐ Enterprise Usage Monitor

Available Functionality	
	<p>*Performance Management Framework - Configured by Performance Management Framework (PMF) Installation.</p> <p>Because the License Information dialog box only displays those products made available by your license key if you are operating under a Legacy license, one or more of the product components in this list may not appear in your installation.</p> <p>If you are operating under a Golden Key license, all product components are selected, by default.</p> <p><input type="checkbox"/> <b>New License Key.</b> This button opens the Update License dialog box, where you can add a new license key and site code. It appears only if you are operating under a Legacy license.</p>

**Reference: Managing Client Licenses**

Access to product features and the number of licensed users is based on your license key and site code.

If you are operating under a Golden Key license, the number of licensed users is unlimited and all product components are available to all users.

If you are operating under a Legacy license, when the number of users exceeds the number of licensed users, the User Licenses Used count displays, in red, a message that the user license count has been exceeded, which is written to the event.log trace file. Users that are authorized to access the Administration Console will receive a message upon signing in.

There are three user license categories:

- ☐ **Total Users.** The total number of named users in the WebFOCUS Repository.
- ☐ **Portal Users.** The number of users with Portal Privileges.

**Notes:**

In the TIBCO WebFOCUS 8.2 Enterprise Edition, users with *only* ReportCaster schedule or Library-only privileges are unlimited. They are not included in the Portal User (PU) count.

In the TIBCO WebFOCUS 8.2 Application Edition, which was discontinued in release WebFOCUS, users with *only* ReportCaster privileges are included in the Portal User (PU) count.

Release 8.0 and 8.1 counts ReportCaster schedule-only and Library-only users in WF Portal user count. Contact support if a customer needs a temporary license key to allow additional WF Portal users. Release 8.2 corrects counting Library-only users. Users with Run within the WebFOCUS Repository Workspaces (/WFC) folder path are counted as Portal users because the Run privilege is used for all item types.

- ❑ **Designer/InfoAssist Users.** The number of users with portal privileges and Designer/InfoAssist privileges.

### **Procedure: How to Configure License Codes**

If you are operating under a Golden Key license, which is the default configuration, access to product features and the number of Managed Reporting users is unlimited. The New License Key button is not available in the License Management dialog box, and this procedure is irrelevant.

If you are operating under a Legacy license, access to product features and the number of Managed Reporting users is based on your license key and site code. You can change these values from the License Management dialog box.

1. In the Administration Console menu bar, select *Licenses*, and then select *TIBCO WebFOCUS Client*.

The License Management window opens, displaying features available under the current license.

2. Select *New License Key*.
3. Enter your new license key and site code.
4. Select *Validate*.

The License Management page displays the current license key, the new license key, and the features that the new license key provides.

5. Select *Save* to implement the new license.

You must reload your web application in order for your changes to take effect. In addition, users must sign out and sign back in to obtain access to any new features.

### **Reviewing User Audit Information**

The User Audit command evaluates the repository license usage for Total Users, Portal Users, and Designer/InfoAssist Users. The command produces a License Analysis report that identifies the total number of licenses by license type, the number of licenses in use by license type, and analyzes license assignments by Group and by User.

You can also run the User Audit utility (license\_audit.bat) from your local WebFOCUS installation directory, which is available in the following location.

For Windows: *drive:\ibi\WebFOCUS82\utilities\mr*

For UNIX or Linux: *install\_directory/ibi/WebFOCUS82/utilities/mr*

in the standard installation, or

For Windows : *drive:\ibi\WebFOCUS\_WFI\WebFOCUS\utilities\mr*

For UNIX or Linux: *install\_directory/ibi/WebFOCUS\_WFI/WebFOCUS/utilities/mr*

in the integrated installation.

The utility generates the License Analysis report and transfers it to the auditUserCounts.htm file, in the same directory.

The License Analysis report contains the following information:

<b>License Analysis</b>	
Edition Name	The name of the current product edition. For example, TIBCO WebFOCUS Enterprise Edition.
Key	Displays your current license key, Golden_Key, by default.
User License	Displays the user license types that are authorized under your current license key. This can include the following: <ul style="list-style-type: none"> <li><input type="checkbox"/> Total Named Users</li> <li><input type="checkbox"/> Portal Users</li> <li><input type="checkbox"/> Designer/InfoAssist Users</li> </ul>
Code	Displays the code for each user license, such as TU for Total Users.
Maximum	Displays the maximum number of user licenses that are available with your license key.
In Use	Displays the number of user licenses that are currently in use.

<b>License Analysis</b>	
Available	Displays the number of user licenses that are not in use for each license type.
<b>Analysis of Groups</b>	
Group Path	<p>Displays the Groups stored in the repository. The following groups are created by the WebFOCUS Repository Creation utility, by default:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> /Administrators</li> <li><input type="checkbox"/> /Anonymous</li> <li><input type="checkbox"/> /EVERYONE</li> <li><input type="checkbox"/> /Managers</li> <li><input type="checkbox"/> /SelfService Developers</li> </ul>
License Type(s)	Displays the license types for each Group, such as TU.
Role	Displays the role of each Group, such as SystemFullControl.
On Resource	Displays the IBFS path to the resource to which the Role is applied for the Group.
Former Type(s)	Displays the former types of licenses for each Group.
Groups Summary	<p>Displays counts for the following:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Number of groups</li> <li><input type="checkbox"/> Number of groups with license types</li> <li><input type="checkbox"/> Number of groups with no license types</li> <li><input type="checkbox"/> Number of groups with changed user types</li> <li><input type="checkbox"/> Number of groups with cleared user types</li> <li><input type="checkbox"/> Number of groups with unchanged types</li> </ul>
<b>Analysis of Users</b>	

<b>License Analysis</b>	
User Name	<p>Displays the users stored in the repository. The following users are created by the TIBCO WebFOCUS Repository Creation utility, by default:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> admin</li> <li><input type="checkbox"/> public</li> <li><input type="checkbox"/> wfdesktop</li> </ul>
License Type(s)	Displays the license types assigned to each user, such as TU.
# Group w/Licenses	Displays the number of groups with licenses of which the user is a member.
First Group with Licenses	Displays the IBFS path to the first group to which the user was assigned.
Former Type(s)	Displays the license types that have been changed or cleared for each user.
User Summary	<p>Displays counts for the following:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Number of users</li> <li><input type="checkbox"/> Number of users with license types</li> <li><input type="checkbox"/> Number of users with no license types</li> <li><input type="checkbox"/> Number of users with changed user types</li> <li><input type="checkbox"/> Number of users with cleared user types</li> <li><input type="checkbox"/> Number of users with unchanged types</li> </ul>

## Understanding TIBCO WebFOCUS Product Editions

Product editions adapt the size and scope of the tools and features available within TIBCO WebFOCUS to match the varying requirements of different types of organizations.

In the 8207 Release, the configuration of product editions depends upon the product offering you maintain.



Customers working with numbered release WebFOCUS and higher use TIBCO WebFOCUS product offerings that feature unlimited access to product components and Administration Console settings using the Golden Key license.

Customers working with releases prior to release WebFOCUS use Legacy product offerings that provide access to product components and Administration Console settings based on the terms of the Legacy license they purchased.

### *Understanding TIBCO WebFOCUS Product Editions*

TIBCO WebFOCUS product offerings, introduced in Release 8207.27.00, support the following product editions:

- ☐ **Basic Edition.** Accommodates up to 50 Named Users.
- ☐ **Standard Edition.** Accommodates up to 500 Named Users.
- ☐ **Enterprise Edition.** Accommodates up to 5000 Named Users.

A Named User is a consumer or author of TIBCO WebFOCUS content who can interact with the software through a dashboard or portal user interface to create or publish content.

The Golden Key license is assigned to each installation, by default, regardless of the product edition. The Golden Key License makes all authoring product components available to all Named Users, by default. A list of these product components appears in the [Reviewing Client License Information](#) on page 77.

Differences between the three product editions in the TIBCO WebFOCUS product offerings are based on the number of users and usage metrics. There is no variation in the range of available products and Administration Console settings.

### *Understanding Legacy Product Editions*

The following legacy product editions are available in releases prior to 8207.27.00.

- ☐ **Application Edition.** Accommodates a minimum of 100 Users with no upper limit.

The Application Edition is a scalable, self-service edition. Starting with a minimum of 100 users, and increasing in groups of ten, it accommodates business users and analysts who can author and deploy highly customized self-service analytical applications to a wide range of non-technical users. The licensing model for the Application Edition is based on seat pricing.

This edition was discontinued in release 8207.27.00.

- ☐ **Enterprise Edition.** Accommodates a minimum of 100 Users with no upper limit.

The Enterprise Edition is a full-scale, completely configurable, self-service edition. It was designed for organizations that want to deploy strategic analytical applications to thousands or even millions of users, including those outside of the organization. It is uniquely suited to scale the deployment of InfoApps to large user populations.

This edition continues to be available in release 8207.27.00.

A unique Legacy License key is assigned to each installation, upon purchase. Access to the product edition purchased by the customer is encoded in the Legacy License key. This Legacy License key makes only those product components purchased by the customer available to Named Users. A list of these product components appears in the [Reviewing Client License Information](#) on page 77.

Differences between the product editions in the Legacy product offerings are based on the number of users and overall usage metrics. There are also two variations in the range of available Administration Console settings.

The Application Edition excludes the following two Administration Console settings:

- ❑ **Anonymous Access.** Located on the Authentication page for each Security Zone listed in the Administration Console Security tab. This setting enables administrators to make the Public user available in their product installation. For more information, see [Anonymous Access](#) on page 227.
- ❑ **Multiple Sign-ins per User.** Located on the Advanced settings page of the Administration Console Security tab. This setting enables users to maintain multiple sessions under the same sign-in, which enables multiple anonymous users to obtain access to system resources simultaneously. For more information, see the *Multiple Sign-ins per User* setting definition in [Using Advanced Settings](#) on page 149.

In the Application Edition, these two settings are not visible and are assigned preconfigured values. However, administrators can customize values in all of the remaining Administration Console settings to conform to the requirements of their organization.

The Enterprise Edition includes the full range of configuration settings, and administrators are able to customize values in all of these settings to conform to the requirements of their organization. Note that even though the Anonymous Access setting is available, it is not activated, by default.

Under the Legacy product offerings, the scope of available product components within a product edition can vary by the Legacy License key configuration. Therefore, the final evaluation of product components made available to an individual user is the list of product components that is visible in the License Information dialog box.

**Procedure: How to Run a User Audit From the Administration Console**

From the Administration Console menu bar, click *Licenses*, and then click *User Audit*.

The License Analysis report opens in a separate browser window.

**Procedure: How to Run a User Audit From the Local TIBCO WebFOCUS Installation Directory**

1. Navigate to the following directory:

For Windows: *drive:\ibi\WebFOCUS82\utilities\mr*

For UNIX or Linux: *install\_directory/ibi/WebFOCUS82/utilities/mr*

2. Double-click the User Audit utility file supported by your operating system:

For Windows: *license\_audit.bat*

For UNIX and Linux: *license\_audit.sh*

3. When prompted, type a valid Administrator ID and press Enter.
4. When prompted, type the password that accompanies the Administrator ID and press Enter.

The batch file generates the report, and stores it in the following location:

On Windows: *drive:\ibi\WebFOCUS82\utilities\mr\auditUserCounts.htm*

On UNIX or Linux: *install\_directory/ibi/WebFOCUS82/utilities/mr/auditUserCounts.htm*

5. Double-click the file *auditUserCounts.htm* to open the License Analysis report.

**Clearing the Cache**

The Clear Cache command refreshes the state of the application by applying saved changes that are not applied dynamically. Even though some changes are dynamic or only require an administrative user to clear the cache to take effect, others require an administrative user to recycle the web application. This activity also clears any data values stored in the Data Values Cache, the Meta Data Cache and the Server Configuration Cache.

The Clear Cache activity also terminates any active searches by closing the existing index readers and index searchers and saves any changes to the Magnify Search interface that were made by updating values in the *collections.xml* file and style sheet files. However, this activity does not close active index writers, nor does it remove existing search results.

**Closing the TIBCO WebFOCUS Administration Console**

When you are working on the WebFOCUS Home page, the Close command closes the Administration Console. After the console closes, you remain signed in as an administrator.

**Note:** This command does not appear on the Administration Console menu bar when you open the Console directly from the Hub. You can close the Administration Console by selecting another option from the side navigation pane.

### Opening TIBCO WebFOCUS Administration Console Help

When you click the Help icon, the online Help file opens to a topic that describes the tab, setting, or feature currently on display.

## Configuring and Customizing Your Environment

You use the Configuration Tab to configure:

- ☐ Client connections to Reporting Servers
- ☐ Application Settings
- ☐ Custom Settings
- ☐ NLS Settings
- ☐ Dynamic Language Switch Settings
- ☐ Redirection Settings
- ☐ InfoAssist Properties

### TIBCO WebFOCUS Reporting Server Settings

To open the TIBCO WebFOCUS Reporting Server Settings, click the *Configuration* tab and expand the *Reporting Servers* folder. You can:

- ☐ Configure basic Client settings for communicating with the Reporting Server.
- ☐ Create or modify an alternate server mapping.
- ☐ Create or modify a Cluster Manager for monitoring server performance statistics and sending requests to the best available server for processing.
- ☐ Manage legacy cluster configurations.

### **Reference:** Reporting Server Node Properties

The Reporting Server Node properties defined in the Basic pane are explained below.

## Basic

### Node Name

The name cannot be the same as any other node name, and it cannot contain more than forty-eight (48) characters. When the client accesses this server, it will use this name.

### Node Description

Optional. The description of the node that appears in the Configuration pane. If this is omitted, the node name will be used.

### Host

The Host name or IP address of the Host Server.

### TCP/IP Port

The Port number for the TCP listener. The default port is 8120.

### HTTP(S) Port

The Port number for the HTTP listener. This is typically one port after the TCP/IP port.

The default HTTP port is 8121.

## Security

The security options for the Reporting Server connection.

- ☐ **Prompt for Credentials.** The Client makes an explicit connection to the Reporting Server with the user ID and password specified in the Web Security tab. This is the default value.
- ☐ **HTTP Basic.** The user ID and password are extracted from the authorization header. These credentials are then used to make an explicit connection to the Reporting Server. You should only select this option when your web tier is performing Basic Authentication.  
  
**Note:** You can verify that the authorization header is available by selecting *HTTP Request Info* in the *Diagnostics* tab.
- ☐ **Kerberos.** The Client passes a Kerberos ticket for the user to the Reporting Server, along with the user ID and group memberships assigned to that user. This option enables an end-to-end single sign on solution from the desktop to the Client, from the Client to the Reporting Server, and from the Reporting Server to supported relational DBMS systems. To use Kerberos authentication, the Reporting Server must run in security OPSYS mode.

- ❑ **SAP Ticket.** The Client passes the user MYSAPSSO cookie, which is created on SAP Enterprise Portal, to the Reporting Server. The Reporting Server then validates the cookie using the SAP security API. This option enables single sign on from the Client to a Reporting Server configured with the Data Adapter for SAP for environments using Open Portal Services in SAP Enterprise Portal.
- ❑ **Service Account.** Allows you to specify a user ID and password to be used for all connections to the Reporting Server.

The service account credentials are encrypted and stored in the SECURITY keyword of the `odin.cfg` file. When defined, the service account overrides any other credentials that may be presented for this Reporting Server node, and all users connect to the Reporting Server using the same credentials. This approach does not make it possible to identify which user is running a given request on the Reporting Server in Managed Reporting deployments, and therefore is not recommended for them.

- ❑ **Trusted.** Allows non-authentication requests to connect to the Reporting Server as trusted. After a user is authenticated through a pre-authentication mechanism or a Sign in page, all subsequent requests to the Reporting Server are trusted.

To use this option, the Reporting Server Security Provider must also be configured to allow trusted connections, and controls should be placed on the Reporting Server to ensure that it rejects connections from unauthorized clients. For example, you should employ the *Reporting Server* `RESTRICT_TO_IP` setting or configure a network firewall so that only your specified clients can connect to the Server.

When you create a new Client Configuration, the *Trusted* option is selected, by default, and the *Pass TIBCO WebFOCUS User ID and their Groups* and *Custom* options appear below it. When you accept the default option, *Pass TIBCO WebFOCUS User ID and their Groups*, the Client passes the ID and group memberships assigned to the user to WebFOCUS Reporting Server. When you select the *Custom* option, the display refreshes to show the *User ID* and the *User's Groups* check boxes allowing you to customize the user information passed to the server. The options *TIBCO WebFOCUS script variable* and *HTTP Header Field* appear under both check boxes, as shown in the following image.

The screenshot shows a configuration window with the following elements:

- ☒ **Trusted**
- ☐ **Pass TIBCO WebFOCUS User ID and their Groups**
- ☒ **Custom**
  - ☒ **User ID**
    - ☒ TIBCO WebFOCUS script variable
    - ☐ HTTP Header Field
  - ☒ **User's Groups**
    - ☒ TIBCO WebFOCUS script variable
    - ☐ HTTP Header Field

Under the *User ID* check box, the *TIBCO WebFOCUS script variable* option displays the `IBIMR_user` parameter, by default. Under the *User's Groups* check box, the *TIBCO WebFOCUS script variable* option displays the `IBIMR_memberof` parameter, by default. You can type over the default values in the TIBCO WebFOCUS script variable options, and type your own values in the HTTP Header Field options.

**Note:** When configuring the Client to make trusted connections to the Reporting Server, you must also enable the Reporting Server to accept trusted connections.

## Advanced

The Reporting Server Node properties from the Advanced pane are explained below.

### Service Name

Contains a description for the Reporting Server node. This description displays to end users.

### Use HTTPS

Enables encrypted communication between the Client and the Reporting Server HTTP listener. The default value is off (check box cleared).

This option must be selected if the Reporting Server HTTP listener is configured to use SSL. If you are using a self-signed certificate to enable HTTPS communication with a Reporting Server, the certificate must be configured in the Java environment where the Client is installed. This enables HTTPS communication between the Reporting Server and the Administration Console.

### Compression

Enables data compression. By default, data compression is disabled.

### Encryption

Sets data encryption ability and the symmetric cryptography method used.

Select one of the following options from the drop-down list:

☐ **0.** Off. This is the default value.

☐ **AES.** Advanced Encryption Standard. The AES selections are in the format

*CIPHER(x) (-MODE)*

where:

*CIPHER*

Is AES128, AES192, AES256.

*x*

Is optional and defines an RSA key length of 1024 bits. When this is not specified, the RSA key is 512 bits.

*CBC*

Is optional and defines the use of Cipher Block Chaining (CBC) mode. When the mode is not specified, Electronic Code Book (ECB) is used.

For example, AES256x-CBC is the AES256 cipher with a 1024-bit RSA key in CBC mode. AES128 is the AES128 cipher with a 512-bit RSA key in ECB mode.

### Connect Limit

Specifies the number of seconds that the Client will hold the pending connection. Other possible values are 0 (no wait) and -1 (infinite wait). The default value is -1.



**Maximum Wait**

Specifies the time, in seconds, that the Client will wait before timeout. You can optionally specify different return times for the first row and other rows. A single number indicates that the return time is valid for any row. If two numbers are separated by a comma, the first number specifies the return time for the first row and the second number specifies the return time for the subsequent rows. The default value is -1, which indicates an infinite wait time.

**Security Object**

For any security option, an administrator can specify one or more HTTP header names and/or cookie names as follows:

- ☐ **Cookie.** Specify each HTTP cookie name separated by a comma (,). For example:

*cookie\_name1, cookie\_name2*

- ☐ **Header.** Specify each HTTP header name separated by a comma (,). For example:

*header\_name1, header\_name2*

**Note:**

- ☐ HTTP cookie and header names must not contain commas (,) or colons (:). These are reserved delimiters.
- ☐ REMOTE\_USER is a special type of HTTP header variable whose contents will not be sent to the Reporting Server. Therefore, it is not a valid HTTP header value. Instead, specify the WF\_REMOTE\_USER variable.

**Basic Cluster Manager Configuration Properties****Node Name**

Is the host name or IP address of the server.

**Node Description**

Optional. The description of the node that appears in the Configuration pane. If this is omitted, the node name will be used.

**Remote CLM Host**

Is the Host name or IP address of the Cluster Manager on which a remote Cluster Manager (CLM) is listening. If more than one address is specified, one of the addresses will be randomly selected until a successful connection to the CLM happens. The number of IP addresses defined in this setting must be the same as the number of port numbers defined in Remote CLM Port. Separate multiple host names or IP addresses with a comma.

### Remote CLM Port

Is the UDP number of the Port on which the Cluster Manager server is listening. The default port is 8200. If more than one port number is specified, the number of port numbers must be the same as the number of IP addresses defined in Remote CLM Host. Separate multiple host names or IP addresses with a comma.

### Security

The security options for the Reporting Server cluster.

- ☐ **Prompt for Credentials.** The Client makes an explicit connection to the Cluster Manager with the user ID and password specified in the Web Security tab. This is the default value.
- ☐ **HTTP Basic.** The user ID and password are extracted from the authorization header. These credentials are then used to make an explicit connection to the Cluster Manager. You should only select this option when your web tier is performing Basic Authentication.

**Note:** You can verify that the authorization header is available in by selecting *HTTP Request Info* in the *Diagnostics* tab.

- ☐ **Kerberos.** The Client passes a Kerberos ticket for the user to the Cluster Manager, along with the user ID and group memberships assigned to that user. This option enables an end-to-end single sign on solution from the desktop to the Client, from the Client to the Cluster Manager, and from the Cluster Manager to supported relational DBMS systems. To use Kerberos authentication, the Cluster Manager must run in security OPSYS mode.
- ☐ **SAP Ticket.** The Client passes the user MYSAPSSO cookie, which is created on SAP Enterprise Portal, to the Cluster Manager. The Cluster Manager then validates the cookie using the SAP security API. This option enables single sign on from the Client to a Cluster Manager configured with the Data Adapter for SAP for environments using Open Portal Services in SAP Enterprise Portal.

- ☐ **Service Account.** Allows you to specify a user ID and password to be used for all connections to the Cluster Manager.

The service account credentials are encrypted and stored in the SECURITY keyword of the odin.cfg file. When defined, the service account overrides any other credentials that may be presented for this Cluster Manager node, and all users connect to the Cluster Manager using the same credentials. This approach does not make it possible to identify which user is running a given request on the Cluster Manager in Managed Reporting deployments, and therefore is not recommended for them.

- ☐ **Trusted.** Allows you to connect to the Cluster Manager with only a user ID. This option is useful when no password is available for the user. Controls should be placed on the Cluster Manager to ensure that connections from unauthorized clients are rejected. For example, you can employ the Cluster Manager RESTRICT\_TO\_IP setting or configure a network firewall so that only a particular client can connect to the Cluster Manager.

When you create a new Cluster Manager Configuration, the Trusted option is selected, by default, and the *Pass TIBCO WebFOCUS User ID and their Groups* and *Custom* options appear below it.

When you accept the default option, *Pass TIBCO WebFOCUS User ID and their Groups*, the Client passes the ID and group memberships assigned to the user to the WebFOCUS Reporting Server. When you select the *Custom* option, additional settings appear and you can customize the user information sent from the Client to the WebFOCUS Reporting Server.

**Note:** When configuring the Client to make trusted connections to the Reporting Server, you must also enable the Cluster Manager to accept trusted connections.

## Advanced Cluster Manager Configuration Properties

### Use HTTPS

Enables encrypted communication between the Client and the HTTP listener.

The default value is off.

This option must be selected if the Cluster Manager HTTP listener is configured to use SSL. If you are using a self-signed certificate to enable HTTPS communication with a Cluster Manager, the certificate must be configured in the Java environment where the WebFOCUS Client is installed. This enables HTTPS communication between the Cluster Manager and the Administration Console.

### Compression

Enables data compression. By default, data compression is disabled.

## Encryption

Sets data encryption ability and the symmetric cryptography method used.

Select one of the following options from the drop-down list:

- ☐ **0.** Off. This is the default value.
- ☐ **AES.** Advanced Encryption Standard. The AES selections are in the format

*CIPHER(x) (-MODE)*

where:

*CIPHER*

Is AES128, AES192, AES256.

*x*

Is optional and defines an RSA key length of 1024 bits. When this is not specified, the RSA key is 512 bits.

*CBC*

Is optional and defines the use of Cipher Block Chaining (CBC) mode. When the mode is not specified, Electronic Code Book (ECB) is used.

For example, AES256x-CBC is the AES256 cipher with a 1024-bit RSA key in CBC mode. AES128 is the AES128 cipher with a 512-bit RSA key in ECB mode.

- ☐ **IBCRYPT.** User-defined IBCRYPT DLL is loaded.

## Connect Limit

Specifies the number of seconds that the Client will hold the pending connection. This is useful in a cluster deployment to avoid a lengthy delay of failover response. Other possible values are 0 (no wait) and -1 (infinite wait). The default value is -1.

## Maximum Wait

Specifies the time, in seconds, that the Client will wait before timeout. You can optionally specify different return times for the first row and other rows. A single number indicates the return time is valid for any row. If two numbers are separated by a comma, the first number specifies the return time for the first row and the second number specifies the return time for the subsequent rows. The default value is -1, which indicates an infinite wait time.

## Security Object

For any security option, an administrator can specify one or more HTTP header names or cookie names as follows:

- ☐ **Cookie.** Specify each HTTP cookie name separated by a comma (,). For example:

*cookie\_name1, cookie\_name2*

- ☐ **Header.** Specify each HTTP header name separated by a comma (,). For example:

*header\_name1, header\_name2*

### Note:

- ☐ HTTP cookie and header names must not contain commas (,) or colons (:). These are reserved delimiters.
- ☐ REMOTE\_USER is a special type of HTTP header variable whose contents will not be sent to the Reporting Server. Therefore, it is not a valid HTTP header value. Instead, specify the WF\_REMOTE\_USER variable.

## Configuring TIBCO WebFOCUS Reporting Server Connections

Reporting Server connection nodes contain all of the information necessary for the Client to connect with and make use of a Reporting Server. A Reporting Server connection node provides access to one server. A Cluster Manager node provides access to multiple servers. Changes you make to the configuration in this section are captured in the *odin.cfg* file, located in *drive:\ibi\WebFOCUS82\client\wfc\etc* on Windows, or located in *install\_directory/ibi/WebFOCUS82/client/wfc/etc* on UNIX or Linux.

The names of all Reporting Server Connection nodes also appear in the Multiple Servers List. This list is located in two places on the Hub. It appears above the Application Directories tree of the Application Directories area and in the Server Administration section of the Management Center area menu.

When you add a Reporting Server Connection node, the name of that node appears on the list. When you delete a Reporting Server Connection node, the name of that node disappears from the list. If you change the name of an existing Reporting Server Connection node, the new name is added, but the name of the existing node remains in the list until you delete the node it represents from the Reporting Server Connections page.

**Procedure: How to Open the WebFOCUS Reporting Server Console From the WebFOCUS Administration Console**

You can make global configuration changes in the server environment by using the Reporting Server Console.

1. In the Administration Console, click the *Configuration* tab. Expand the *Reporting Servers* folder and expand the *Server Connections* folder.

The existing Reporting Servers are shown.

2. Right-click a Reporting Server node, and click *Reporting Server Console*.

If you are prompted to sign in, type the credentials of the Reporting Server Administrator.

The Reporting Server Console opens in a separate window.

For more information about the Reporting Server Console, see the *Server Administration* manual, or click *Help*.

**Procedure: How to Add a WebFOCUS Reporting Server Server Connection**

1. In the Administration Console, click the *Configuration* tab, and expand the *Reporting Servers* folder.
2. Right-click the *Server Connections* folder and click *New*.

The Client Configuration pane opens.

3. In the Client Configuration pane, type the node name, host, and TCP/IP port. You can optionally specify a node description and HTTP(S) port.

**Note:** The name cannot be the same as any other node name, and it cannot contain more than forty-eight (48) characters. When the client accesses this server, it will use this name.

4. Select the type of security to use when connecting to this Reporting Server.

- ☐ If you select *Prompt for Credentials* or *HTTP Basic*, proceed to step 8.

**Note:** If you are using HTTP Basic authentication, you can verify the authorization header by selecting *HTTP Request Info* in the *Diagnostics* tab.

- ☐ If you select *Kerberos* or *SAP Ticket*, proceed to step 8.

**Note:** See [Configuring Kerberos for Single Sign On](#) on page 256 for additional setup requirements.

- ☐ If you select *Service Account*, proceed to step 5.

- ☐ If you select *Trusted*, proceed to step 6.

*Trusted* is the default. This is the recommended approach to connect to a Reporting Server.

5. If you selected *Service Account*, type the Service Account ID and password, then proceed to step 8.
6. If you selected *Trusted*, configure the behavior of the trusted connection between the Client and the Reporting Server:
  - ☐ If you would like to pass the user ID and group information to the Reporting Server using the `IBIMR_user` and `IBIMR_group` script variables respectively, proceed to step 8. This is the default behavior.
  - ☐ If you would like to pass only the user ID, or to pass the user ID and/or group information with a different variable name or using HTTP headers instead of script variables, select the *Custom* radio button and proceed to step 7.
7. If you selected *Trusted - Custom*, customize the information sent to the Reporting Server, and the script variables or HTTP headers used.
  - a. User ID is pre-selected. Select *TIBCO WebFOCUS script variable* or *HTTP Header field*, depending on how you will pass user IDs. Accept the default script variable, `IBIMR_User`, or type an alternative script variable or HTTP Header field.
  - b. If you would like to pass group information to the Reporting Server, select *User's Groups*, then select *TIBCO WebFOCUS script variable* or *HTTP Header field*, depending on how you will pass group information. Accept the default script variable, `IBIMR_memberof`, or type an alternative script variable or HTTP Header field.

For more information on using TIBCO WebFOCUS script variables and HTTP headers, see [Manipulating TIBCO WebFOCUS Variables](#) on page 707. For more information on configuring trusted connections on the Reporting Server, see [Configuring Trusted Connections](#) on page 49.

8. Optionally, expand the *Advanced* section to customize the properties for service name, Use HTTPS, Compression, Encryption, Connection Limit, Maximum Wait, and Security Object. If left blank, these options use the default properties.

**Note:** When configuring the Client to make trusted connections to the Reporting Server, you must also enable the Reporting Server to accept trusted connections.

For more information about the *Advanced* settings, see [Reporting Server Node Properties](#) on page 88.

9. Click **Save**.

A node for the new WebFOCUS Reporting Server connection appears in the tree under the Server Connections folder. The name of the new WebFOCUS Reporting Server connection also appears in the Multiple Servers List. This list is located in two places on the Hub. It appears above the Application Directories tree of the Application Directories area and in the Server Administration section of the Management Center area menu.

### **Procedure: How to Modify a WebFOCUS FOCUS Reporting Server Connection**

1. In the Administration Console, click the *Configuration* tab, and expand the *Reporting Servers* folder.
2. Click the server connection you would like to modify.  
The connection properties appear in the Client Configuration pane.
3. Make the desired changes and click *Save*.

### **Procedure: How to Configure Encrypted Communication with a WebFOCUS Reporting Server**

This procedure assumes that you have already successfully installed and configured the WFServlet implementation.

1. If you are using Sun JVM with an encryption cipher key that is over 128 bits, be sure to install the Java Cryptography Extension (JCE). You can obtain the JCE from the Oracle download website.  
**Note:** The JCE must be installed in the JVM directory that your application is using. For more information, see the *JCE* documentation.
2. Redeploy the webfocus.war file if it is necessary to point to the .war file. Otherwise, point to the web application directory.
3. In the Administration Console, expand the *Reporting Servers* folder, then expand the *Server Connections* folder.
4. Select the Reporting Server node (for example, *EDASERVE*) you want to configure for encryption.  
The Client Configuration pane appears.
5. Click the *Advanced* arrow to open the Advanced section.
6. Click the encryption cipher you want to use from the Encryption list.



**Note:** When using any of the AES encryption ciphers, the client randomly generates a new RSA key pair (public and private keys of the specified length) and sends the public key to the server. Upon receipt of the public key, the server generates a random secret key. The length of the secret key depends on the chosen cipher strength. The secret key is encrypted with the public RSA key and sent back to the client, which decrypts it with its private RSA key. After the exchange, the client and the server both share the same secret key, and use it to encrypt and decrypt all communication between them.

7. Click **Save**.

### **Procedure: How to Set a Default WebFOCUS Reporting Server Node**

Selecting a default Server node in the Configuration tab sets the node as the IBI\_REPORT\_SERVER value in the webfocus.cfg file. However, if a site profile, universal profile, or request URL specifies a different default Server node, that value will override this selection. Profiles and request URLs use the IBIC\_server setting for that purpose.

1. In the Administration Console, on the *Configuration* tab, expand the *Reporting Servers* folder, and then expand the *Server Connections* folder.
2. Right-click a Reporting Server node, and then click *Set as Default*.

A green check mark appears on the server icon indicating the default node.

### **Procedure: How to Test a WebFOCUS Reporting Server Connection**

1. In the Administration Console, on the Configuration tab, expand *Reporting Servers*, and then expand *Server Connections*.
2. Right-click the connection you want to test, and point to *Test*.
  - ☐ Select *TABLE Request* to test a table query on the server.
  - ☐ Select *GRAPH Request* to test a graph query on the server.
  - ☐ Select *Stored Procedure* to test a stored procedure on the server.
3. On the test page, click *Run*.
4. If the *Valid credentials are required for reporting server* page opens, enter your User ID and Password, and then click *Sign in*.
5. Review the test results.

If you receive a Reporting Server Error message, the server connection failed.

If a page opens, displaying the results of your test, the server connection was successful.

6. When your review of the results is complete, close the results page, and on the test page, click *Cancel*.

### Reconnecting the Client to the Repository

Whenever a network, operating system, relational database system, or Application Server disruption temporarily disconnects the Client from the Repository, the Client automatically reconnects to the Repository as soon as the disruption is resolved. There is no need to stop and restart the Application Server to re-establish the connection between the Client and the Repository.

If you are able to remain signed in to a session during the disruption, you will automatically reconnect to the Repository as soon as the connection is restored. If the disruption forces you to sign out, you will automatically reconnect to the Repository when you sign in again. After the connection is restored, you can resume your work from the point at which you were interrupted.

Records of the events that disrupt and restore the connection between the Client and the Repository are captured in the System log.

### Alternate Server Mapping

You can configure Alternate Server nodes for use with the Managed Reporting Deferred Receipt feature.

Deferred Receipt requests can be processed by using the immediate Reporting Server (immediate server) or by using an alternate deferred receipt server (Deferred Server) dedicated to running only deferred requests. The resources for the Deferred Server are managed independently from the immediate server. The Deferred Server must have the same access to applications, data sources, and Master Files, and run in the same environment (for example, UNIX), as the immediate server.

**Note:** If you use the Reporting Server for z/OS, additional configuration is required to use deferred requests. You must set up an alternate server or service to handle deferred requests and then configure the WebFOCUS Client to send requests to that server by setting up a deferred server mapping. For more information, see the *Installation and Configuration for Windows* manual for your platform.

### **Procedure:** How to Add an Alternate Server Mapping

1. In the Administration Console, on the Configuration tab, expand the *Reporting Servers* folder.
2. Right-click the *Alternate Server Mapping* folder and click *New*.

The Alternate Server Mapping pane opens.

3. Click the main server in the Server list.
4. Click the alternate server from the Alternate Server list.
5. Click Save.
6. When you receive the Successfully Saved message, click OK.

**Procedure: How to Modify an Alternate Server Mapping**

1. In the Administration Console, on the Configuration tab, expand the *Reporting Servers* folder, and then expand the *Alternate Server Mapping* folder.
2. Click the node of the server mapping you would like to modify.

The connection properties appear in the Client Configuration pane.

3. Make the desired changes and click Save.

**Note:** Changes to the main server value automatically clear the value assigned to the alternate server. Therefore, if you change the value in the main server setting, you must also select an alternate server.

4. When you receive the Successfully Saved message, click OK.

**Procedure: How to Map a Deferred Server Node to an Immediate Server Node**

Using the Administration Console, add a node for the deferred server the same way as adding a non-deferred node. Next, perform the following steps to map the Deferred Server to an immediate Server node:

1. In the Administration Console, on the Configuration tab, expand the *Reporting Servers* folder and right-click *Alternate Server Mapping*.
2. Click *New* to create a new mapping.

The Alternate Server Mapping page opens, allowing you to edit the altdnode.wfs file.

3. Click the name of the immediate server in the Server list, which displays the list of all available Reporting Servers.
4. Click the name of the deferred server in the Alternate Server list, which displays the list of all available Reporting Servers (excluding the immediate server you just specified).
5. Click Save.

**Note:** You can map multiple immediate servers to the same deferred server by repeating these steps.

## Managing Clustered Servers

Clustering allows you to automatically send requests to the best available server for processing.

The Cluster Manager (CLM) enables you to define clusters of Reporting Servers that can be brought up and down as needed. In addition, the Cluster Manager enables you to configure cluster properties, including response time and dispatch method. It then monitors cluster performance and provides statistics, such as the average response time for requests, the number of connection failures and errors, and how many requests were sent per minute.

For more information, see [Reporting Server Node Properties](#) on page 88.

### **Procedure:** How to Add a Cluster Manager Node

This procedure details the steps you take to create a cluster of servers in a node using the Cluster Manager.

1. In the Administration Console, on the Configuration tab, expand the *Reporting Servers* folder.
2. Right-click the *Cluster Manager* folder and click *New*.

The Cluster Manager Configuration pane opens.

3. In the Cluster Manager Configuration pane, type the Node Name, Remote CLM host, and Remote CLM port. You can optionally specify a Node Description.

The default Remote CLM Port is 8120.

**Note:** The Node Name provided in the Administration Console for Cluster Manager configurations must match the Cluster name of the Cluster Manager Reporting Server.

4. Select the type of security to use when connecting to this Cluster Manager:
  - ☐ If you select *Prompt for Credentials*, *HTTP Basic*, *Kerberos*, or *SAP Ticket*, click the appropriate option and proceed to step 7.
  - ☐ If you select *Service Account*, proceed to step 5.
  - ☐ If you select *Trusted*, proceed to step 6.

**Note:**

- ☐ If you are using HTTP Basic authentication, you can verify the authorization header by selecting *HTTP Request Info* in the *Diagnostics* tab.
- ☐ If you are using Kerberos authentication, see [Configuring Kerberos for Single Sign On](#) on page 256 for additional setup requirements.

5. If you selected *Service Account*, enter a user ID and password. Proceed to step 7.
6. If you selected *Trusted*, by default, the client passes the user ID and group information to the Reporting Server using the IBIMR\_user and IBIMR\_group script variables. You can customize this behavior by using the different variable names, using HTTP headers instead of script variables, or not passing group information.
  - a. If you would like to enable the default behavior, select *Pass WebFOCUS User ID and their Groups* and proceed to step 7.
  - b. If you would like to use a TIBCO WebFOCUS script variable or HTTP header to pass user or group information, select *Advanced*.
  - c. User ID is pre-selected because you will always send user information. Select *TIBCO WebFOCUS script variable* or *HTTP Header field*, depending on how you will pass user IDs. Accept the default script variable, IBIMR\_User, or type an alternative script variable or HTTP Header field.
  - d. If you would like to pass group information to the Reporting Server, select *User's Groups*, then select *TIBCO WebFOCUS script variable* or *HTTP Header field*, depending on how you will pass group information. Accept the default script variable, IBIMR\_memberof, or type an alternative script variable or HTTP Header field.

**Note:** You must configure the security provider on the Reporting Server to accept trusted connections.

For more information on using TIBCO WebFOCUS script variables and HTTP headers, see [Manipulating TIBCO WebFOCUS Variables](#) on page 707. For more information on configuring trusted connections on the Reporting Server, see [Configuring Trusted Connections](#) on page 49.

7. If you are using the default service name, use of SSL, compression, encryption, connection limit and wait time, and are not using cookies or headers, proceed to step 8. If you would like to customize these properties, expand the *Advanced* arrow and configure the desired fields.
8. Click *Save*.

### **Procedure:** How to Modify a Cluster Manager Node

1. In the Administration Console, on the *Configuration* tab, expand the *Reporting Servers* folder, and then expand the *Cluster Manager* folder.
2. Right-click the node you want to edit and click *Edit*.  
The node properties appear in the Cluster Manager Configuration pane.
3. Make the desired changes and click *Save*.

## Managing Legacy Cluster Configurations

Previous implementations of Server clustering are still supported through the Legacy Cluster Configuration screen.

### **Procedure:** How to Configure a Legacy Cluster

1. In the Administration Console, on the *Configuration* tab, expand the *Reporting Servers* folder.
2. Right-click the *Legacy Cluster Configuration* folder and select *New*.  
The Legacy Cluster Configuration pane opens.
3. Type a Node Name and, optionally, a Node Description.
4. Select the servers to include in the cluster as follows:
  - ☐ Click a single server in the Available list box, and click the right arrow.
  - ☐ Hold down the Ctrl key, click multiple non-adjacent servers, and click the right arrow.
  - ☐ Hold down the Shift key and click on the first and last adjacent server to include all of them, and click the right arrow.
5. Click *Save*.

## Using Client Profiles

Client variables are not passed to the Reporting Server, so they cannot be included directly in any of the Reporting Server profiles (edasprof.prfl, user profiles, and group profiles). However, you can make use of Client variables by specifying procedures in the site profile or universal profile. The site profile and the universal profile run after the Reporting Server profile processing, but before the report request. The site profile executes from the Client and the universal profile executes code from both the Client and the ReportCaster Distribution Server.

The site profile and the universal profile can also be added directly to webfocus.cfg or site.wfs.

## The Client Site Profile

A site profile is sent to the Reporting Server by the Client and is executed on the Reporting Server immediately after all Reporting Server profiles. It can override settings in the Reporting Server profiles and can take advantage of the variable values set by the other profiles. This makes the amper variables exported by the Client with the (pass) syntax available for use on the Reporting Server.

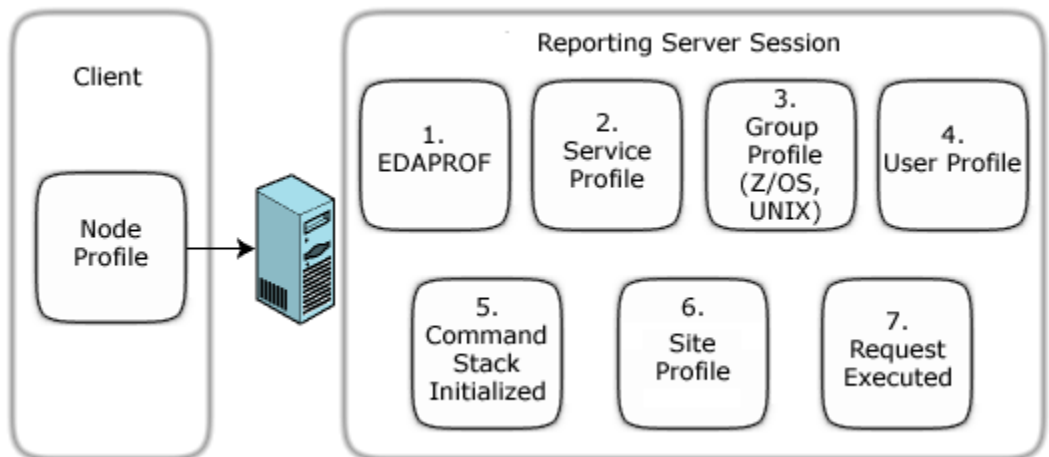
For more information on using amper variables, see [Manipulating TIBCO WebFOCUS Variables](#) on page 707. For more information on Reporting Server profiles, see [TIBCO WebFOCUS Reporting Server Profiles](#) on page 56.

Customers can use a site profile to:

- ❑ Make a series of data source connections dependent on a variable sent from the Client.
- ❑ Use a Client variable (for example, &REMOTE\_ADDR or &IBIMR\_user) in a custom security procedure on the Reporting Server, which can set other amper variables that affect subsequent report processing. This is an example of application-based security.

**Note:** The site profile is only processed when procedures are run by the Client. Use the universal profile to include commands to be processed when procedures are run by the ReportCaster Distribution Server.

The following diagram illustrates site profile processing. The numbers associated with the files refer to the order in which the files are processed.



### **Procedure:** How to Create a Site Profile

1. In the Administration Console, on the *Configuration* tab, under the Application Settings folder, click *Client Settings*.
2. Type the name of the desired procedure in the Site Profile (IBI\_SITE\_PROFILE) field.

The Site Profile (IBI\_SITE\_PROFILE) field uses the following syntax:

`_site_profile=command`

where:

`command`

Is any valid Reporting Server syntax.

Once you have completed these steps, the profile procedure or procedures run automatically. There is no need to restart the Server.

### The Universal Profile

A universal profile is sent to the Reporting Server by both the Client and the ReportCaster Distribution Server and is executed on the Reporting Server. It runs immediately following all Reporting Server profiles.

Unlike the site profile, the universal profile is included during the execution of procedures by ReportCaster. Therefore, it should not include any logic or constructs that will execute only on the Client. For example, HTTP header variables should not be included, because they are available to the Client but not to the ReportCaster Distribution Server.

#### **Procedure:** How to Create a Universal Profile

1. In the Administration Console, on the Configuration tab, under the Application Settings folder, click *Client Settings*.
2. On the Client Settings page, type the desired procedure in the Universal Profile (IBI\_UNIVERSAL\_PROFILE) field.

The Universal Profile (IBI\_UNIVERSAL\_PROFILE) parameter uses the following syntax:

`IBI_UNIVERSAL_PROFILE=command`

where:

*command*

Is any valid Reporting Server syntax. The universal profile is executed by both the Client and the ReportCaster Distribution Server. This differs from the Site Profile, which is only executed by a Client request.

Once you have completed these steps, the profile procedure (or procedures) run automatically. There is no need to restart the Server.



## Managing Distribution Directories

The Distribution Directories folder contains a configuration of distribution directory nodes that supports scheduled report distributions from ReportCaster. Distribution directory nodes specify those folders within the IBFS FILE subsystem that capture output from scheduled report distributions, and can be mapped to existing file system directories that are accessible to the ReportCaster Distribution Server, as shown in the following image.

The screenshot shows the 'Configuration' tab of the TIBCO WebFOCUS Client. The left sidebar lists the following configuration items: Alternate Server Mapping, Cluster Manager, Legacy Cluster, Distribution Directories (selected), and Application Settings. The main area is titled 'Network Location' and contains three required fields: 'Name' (text input), 'Type' (radio buttons for 'Path' and 'Server', with 'Path' selected), and 'Path' (text input). 'Save' and 'Cancel' buttons are located at the bottom right.

When using the Repository method, the ReportCaster Distribution Server delivers scheduled report output to these IBFS FILE subsystem folders and their associated network locations or FTP server locations. The output is then available for use by other tools or applications that can retrieve it from the designated network or FTP server location.

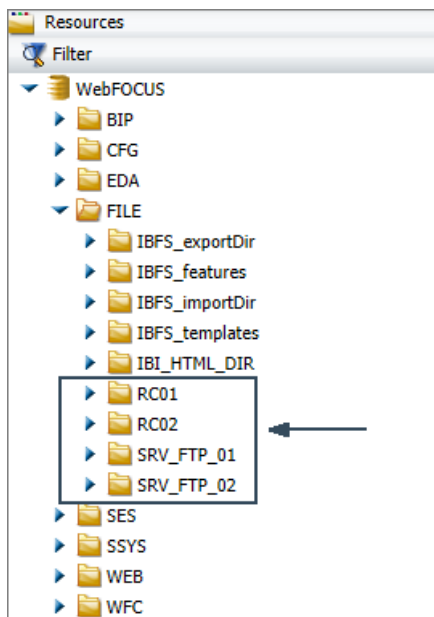
Because they are folders within the IBFS FILE subsystem, distribution directory nodes are subject to the same security configuration as any other IBFS resource. Administrators can therefore use distribution directory nodes to limit the availability of the IBFS files that support scheduled report distributions to a selected set of authorized groups and users.

The Network Location page opens when you open a new or existing distribution directory node. This page contains the following fields:

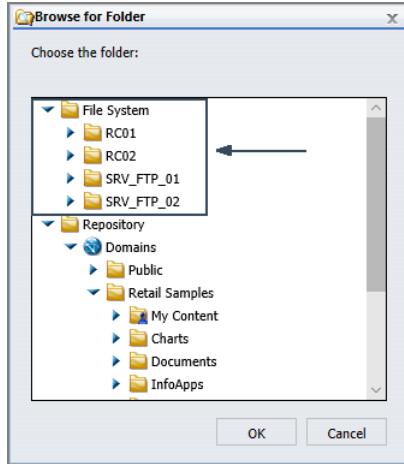
### Name

The Name field identifies the name of a distribution directory node within the IBFS FILE subsystem. The value you assign to this field must be unique. You receive an error if you attempt to create more than one distribution directory node with the same name.

The value you assign to the Name field appears on the folder that represents the distribution directory node in the Resources tree. When the Resources tree on the Legacy home page is displayed in Full View mode, folders for distribution directory nodes appear under the FILE subsystem folder, as shown in the following image.



The value you assign to the Name field also appears on folders that represent distribution directory nodes in the Browse for Folder dialog box that opens from the Distribution dialog box of the ReportCaster Basic Scheduling Tool and Advanced Scheduling Tool, as shown in the following image. Administrators and authorized users can see these folders when they configure a Report Distribution schedule that uses the Repository method.



### Type

The Type field allows administrators to select the type of distribution method and external connection to be supported by a new distribution directory. There are two options:

**Path.** When this option is selected, the new IBFS distribution directory node will be connected to a directory that is accessible to the Distribution Server. The Path field remains on display in the Network Location page and contains the path to that directory.

**FTP Server.** When this option is selected, the new IBFS distribution directory node will be connected to an FTP server identified by a predefined FTP setting configuration maintained in ReportCaster. The Path field is replaced by the Server field with its list of predefined FTP Setting configurations.

Distribution directory nodes can only support a single connection type. Therefore, this field is visible only when creating new distribution directory nodes. It is not visible in distribution directory nodes that have already been created.

In addition, because the option to assign a distribution directory node to an FTP server is possible only when predefined FTP Connection setting configurations are available, this field, and the two options it contains, appears only when at least one predefined FTP Setting configuration, in addition to the (Default Setting) configuration, is available in ReportCaster. For more information about FTP Setting configurations, see the *ReportCaster* technical content.

## Path

The Path field identifies the path to the network location that corresponds to a distribution directory node in the IBFS system, as shown in the following image. Because this location is the file system target of the scheduled report output, the Distribution Server must be able to write files to the location defined by this path. Within this limitation, the path can identify any location that supports your requirements.

The screenshot shows a web-based configuration interface. At the top, there are tabs: Configuration (selected), Security, ReportCaster, and Diagnostics. On the right side of the top bar are links for Licenses, Clear Cache, and a help icon. The left sidebar shows a tree view under 'Configuration' with 'Reporting Servers' and 'Distribution Directories'. Under 'Distribution Directories', 'RC01' is selected. The main content area is titled 'Network Location' and contains two required fields: 'Name' with the value 'RC01' and 'Path' with the value '\\Server01\\ReportOu'. Below these fields are 'Save' and 'Cancel' buttons.

The format of a path assigned to this value must conform to the requirements of the operating system used by the Distribution Server or to the requirements of the Universal Naming Convention (UNC). For example, you could use one of the following paths to identify a file system directory named ReportOutput\\Report01, that is located on a server named Server01, which, in a Microsoft Windows-based network, is mapped to the drive letter W:\\.

- ☐ For Windows: W:\\ReportOutput\\Report01
- ☐ For UNIX or Linux: /ReportOutput/Report01
- ☐ For the Universal Naming Convention: \\Server01\\ReportOutput\\Report01

If a path uses a format that is accessible to the Application Server as well, full details of the results of the file distribution are available for review from the Application Server.

If a path points to a directory on a machine that does not host the Application and Distribution Servers, both the Application Server, typically Tomcat, and the Distribution Server must be running under a user ID that has permission to access the directory. The Application Server must at least have Read permission to the targeted directory. The Distribution Server must have Read/Write permission to the targeted directory. The configuration of these permissions takes place within the external network, and is beyond the scope of this document.

Note that you must define the path to the file system location before you can create a distribution directory node for it. If the path in a distribution directory node does not point to an existing network location, the distribution directory is invalid and cannot support a scheduled report distribution.

### FTP Server

The FTP Server field identifies the predefined FTP Setting configuration to which a distribution directory node is mapped in the IBFS system, as shown in the following image.

The screenshot shows the 'Configuration' tab in the TIBCO WebFOCUS console. On the left, a tree view under 'Distribution Directories' lists 'RC01', 'RC02', 'SRV\_FTP\_01' (selected), and 'SRV\_FTP\_02'. The main panel, titled 'Network Location', contains two required fields: 'Name:' with a text input containing 'SRV\_FTP\_01' and 'FTP server:' with a dropdown menu showing 'FTP\_01'. 'Save' and 'Cancel' buttons are at the bottom right.

The list of servers in this field is limited to the set of predefined FTP server configurations available in the ReportCaster Console Configuration tab. The list excludes the default FTP Server configuration defined within ReportCaster because it is not a true IBFS node. It also excludes any user-defined FTP configurations attached to FTP Distribution schedules. In order to include the configurations defined in either of these locations, administrators must create a duplicate pre-defined FTP Setting configuration within ReportCaster.

The details of an FTP Server configuration identify the name of the FTP server to which the connection is made, the authorized User ID and Password for that FTP server, and the security protocol it uses. For more information about the FTP Settings configuration, see the *ReportCaster* technical content.

When creating a new distribution directory node, this setting appears only after you click the Server option in the Type setting.

When working with an existing distribution directory node, this setting appears only if the distribution directory node was configured to support an FTP Server connection when it was created.

## Granting Access to Distribution Directory Nodes

Just as the ability to distribute scheduled report output using the Repository method is typically limited to administrators, and to those users in the Developers and Advanced Users groups who are authorized to create, edit, and distribute content within their assigned workspaces, the ability to access distribution directory nodes that support scheduled report distributions to the FILE subsystem should be limited to administrators, and to the users who are authorized to distribute the scheduled report output they contain. Using the tools of the workspace-based security model, administrators can ensure that distribution directories are available only to these authorized users.

In order to make distribution directories fully accessible to authorized users, administrators must do the following:

1. Ensure that the ability to access resources in the IBFS FILE subsystem folder is available to users in authorized groups.
2. Make the ability to distribute scheduled report output to the File System available to users in authorized groups.
3. Make individual distribution directory nodes available to the groups that must use them to contain report output created from scheduled report distributions.

These requirements call for the assignment of the existing List Role to the FILE folder in the IBFS system, and the creation of two new roles: a role that grants access to the file system distribution method, referred to as the Distribution to File System role, and a second role that grants access to the privileges required to create or overwrite scheduled report content in a distribution directory, referred to as the Distribution Directory Access role.

A rule that makes the List role available to all users in the EVERYONE group is assigned to the FILE folder, by default. This rule must be assigned to the FILE folder in order to make Distribution Directory nodes, which exist within the IBFS FILE subsystem available to authorized groups and users.

The Distribution to File System role is designed to grant users the Distribute to File System (opDistributeFileSystem) privilege when working with a workspace. This role can include additional privileges, if required, or administrators can add this privilege to an existing role that contains other privileges. However, by creating a dedicated role limited to file system distribution access, administrators can achieve the most effective control over this role and its use.

The Distribution Directory Access role is designed to grant users the additional access needed to work with individual distribution directory nodes. It consists of the Access Resource (opList) privilege that enables users to see the distribution directory node and its contents, the Create Items (opCreateItem) privilege that enables users who own reporting schedules to create files containing scheduled report output in the distribution directory node, and the Edit Items (opWrite) privilege that enables users who own reporting schedules to overwrite files containing scheduled report output in the distribution directory if the previous version of that file did not use a unique filename that includes a timestamp. The Create Items and Edit Items privileges are required because the Distribution Server that produces the scheduled report output signs into WebFOCUS with the ID of the user that owns the reporting schedule in order to transfer scheduled report output to the distribution directory node.

As with the File System Distribution role, this role can include additional privileges, if required, or administrators can add these privileges to an existing role that contains other privileges. However, by creating a dedicated role limited to the ability to create and view content in a distribution directory node, administrators can achieve the most effective control over this role and its use.

Administrators must also create distribution directory nodes for those workspaces that generate scheduled report output. If all members are permitted to see or generate scheduled report output from a workspace, a single distribution directory node can accommodate all output from that workspace. However, if access to sensitive or confidential report output from a workspace must be restricted to a smaller group, additional distribution directories that are limited to these smaller groups may be required.

In order to complete the configuration required to make distribution directories available to authorized users, administrators must create rules for the workspaces and distribution directories that support scheduled report output distribution to the IBFS File subsystem. They must create a Distribution to File System rule for each workspace that generates scheduled report output for delivery to the File System in order to allow group members in that workspace to access the File System folder and workspace directory subfolders when they create a schedule. They must also create a Distribution Directory Access rule for each distribution directory node that contains scheduled report output in order to allow group members from the workspace that generated the scheduled report output to access that distribution directory and create scheduled report output in it.

We recommend that administrators configure distribution directory nodes in the following task sequence:

1. Identify the workspaces and groups that require access to distribution directories for scheduled report output.
2. Ensure that all users who need to run scheduled reports are included in the groups that must have access to the scheduled report output.

3. Create a Distribution to the File System role.
4. Create a Distribution Access role.
5. Create the distribution directory nodes required to contain the scheduled report output generated by each workspace.
6. Create a Distribution to File System rule for each group that generates scheduled report output for distribution to the file system.
7. Create a Distribution Directory Access rule for each group assigned to a distribution directory node that contains scheduled report output from their workspace.

Tasks one and two are not included in the topics that follow. They require an assessment that can only be made by each administrator based on the requirements of their organization. The remaining tasks are described in detail in the topics that follow.

### ***Procedure:*** How to Create a Distribution to the File System Role

This role is designed to grant the privilege to distribute scheduled report output from a workspace to the IBFS File subsystem. We recommend that this role be limited to a single privilege and be identified by that privilege as described in this procedure. However, this role can include additional privileges if required, or the Distribute to File System (opDistributeFileSystem) privilege can be assigned to an existing role.

1. Sign in as an administrator, and open the Security Center.
2. In the Security Center, click the *Roles* tab.
3. Click *New Role* to open the New Role dialog box.
4. In the Name field, type a name for this new role. For example, Distribution to the File System.
5. Under the Scheduling and Distribution privilege category folder, select the *Distribute to File System* check box.
6. Click *OK* to save the new role.

The Distribution to the File System role appears in the Roles list.

### ***Procedure:*** How to Create a Distribution Directory Access Role

This role is designed to grant the privilege to access distribution directory nodes and create and overwrite scheduled report output in them. We recommend that this role be limited to the Access Resource, Create Item, and Edit Item privileges and be identified as a distribution directory access role as described in this procedure. However, this role can include additional privileges if required, or these privileges can be assigned to an existing role.

1. Sign in as an administrator, and open the Security Center.



2. In the Security Center, click the *Roles* tab.
3. Click *New Role* to open the New Role dialog box.
4. In the Name field, type a name for this new role. For example, Distribution Directory Access.
5. Under the Basic Reporting privilege category folder, select the *Access Resource* check box.
6. Under the Application Development privilege category folder, select the *Create Items* check box and select the *Edit Items* check box.
7. Click *OK* to save the new role.

The Distribution Directory Access role appears in the Roles list.

**Procedure: How to Create a Distribution to File System Rule for a Workspace**

A Distribution to File System rule grants access to the IBFS File subsystem to those groups assigned to a workspace that uses ReportCaster to distribute scheduled report output. Before you begin, make sure that all users who need access to the File subsystem are assigned to those groups to which this rule is assigned.

1. Sign in as an administrator, and open the Workspaces view.
2. In the Resources tree, under the Workspaces node or in the content area, right-click the workspace that requires the use of the File System distribution method for scheduled report content, point to *Security*, and then click *Rules* to open the Security Rules dialog box.
3. On the Users and Groups tab, click the name of the Group that must have access to the File System Distribution Method.
4. In the Rules for Group list, click the name of the role you created for distribution directory access. For example, *Distribution to File System*.
5. In the Access column of the Distribution to File System role entry, click *Permitted*, and in the Apply To column, accept the default value, Folder and Children.
6. Click *Apply* and then click *OK* to save the new rule.
7. Repeat steps 3 through 6 to create the Distribution to File System rule for any additional workspaces or groups.

**Procedure: How to Test the Assignment of a Distribution to File System Rule to a Workspace**

1. Sign in with the user ID and password of a member of a group to which the Distribution to File System rule was assigned, and open the Workspaces view.
2. Right-click a report in the workspace, point to *Schedule*, and then click *Repository* to open the ReportCaster Distribution Scheduler wizard.

3. Click *Folder Location* to open the Browse for Folder dialog box.
4. If the File System folder appears at the top of the Choose the folder tree, click *OK* and close the ReportCaster Distribution Scheduler wizard.
5. If the File System folder does not appear, click *Cancel*, close the ReportCaster Distribution Scheduler wizard, and perform the following steps.
  - a. Right-click the workspace, point to *Security*, and click *Rules on this Resource* in order to determine if the Distribution to File System rule is assigned to the group under which you signed in, and if it was not, assign the rule to the group.
  - b. Ensure that the List role is assigned to the FILE subsystem folder for the EVERYONE group.

**Procedure: How to Create a Distribution Directory Node**

When creating a node for a distribution directory, you must type a path to an existing network location. You cannot create a new network path merely by typing it in this field and saving the distribution directory node. If the path does not point to an existing network location, the distribution directory node is invalid and cannot support a scheduled report distribution.

1. On the Administration Console Configuration tab, right-click the *Distribution Directories* folder, and then click *New* to open the Network Location page.
2. In the Name field, type the name that identifies the new distribution directory node.
3. To create a distribution directory node that connects to a network location, perform the following steps:
  - a. Click *Path* in the Type field.
  - b. In the Path field, type the path to the existing network location that corresponds to the distribution directory node in the IBFS system using one of the following formats.

For Windows:

*drive:\path*

For UNIX or Linux:

*/path*

For the Universal Naming Convention:

*\\server\path*

where:

*drive*

Is the letter that represents the drive to which the server is mapped.

*server*

Is the name of the server that hosts the directory to which scheduled reports for the node identified in the Name field are to be directed.

*path*

Is the name of the network path to the directory to which scheduled reports for the node identified in the Name field are to be directed.

For example:

- ☐ For Windows: W:\ReportOutput\Report01
- ☐ For UNIX or Linux: /ReportOutput/Report01
- ☐ If using the Universal Naming Convention: \\Server01\ReportOutput\Report01

- c. Continue with step 5.
4. To create a distribution directory node that connects to an FTP Server, perform the following steps:
  - a. Click *Server* in the Type field.
  - b. Click the name of the predefined FTP Setting configuration that corresponds to the distribution directory node in the IBFS system.
  - c. Continue with step 5.
5. Click *Save As*.
6. If you receive a message warning you to enter all required information, click *OK*, and type and save the required information as described in steps 2 through 4.
7. If you receive a message stating that the node was successfully saved, click *OK*.

The Network Location page closes, and a node for the new distribution directory appears under the Distribution Directories folder.

**Procedure: How to Create a Distribution Directory Access Rule for a Distribution Directory Node**

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, expand the *Distribution Directories* folder.
3. Right-click the distribution directory node you wish to update, point to *Security*, and then click *Rules* to open the Security Rules dialog box.
4. On the Users and Groups tab, in the Groups list, click the name of the group that must have access to the distribution directory node.
5. In the Rules for Group list, click the name of the role you created to make distribution directory nodes accessible. For example, *Distribution Directory Access*.

6. In the Access column of the Distribution Directory Access role entry, click *Permitted*, and in the Apply To column, accept the default value, Folder and Children.
7. Click *Apply* and then click *OK* to save the new rule.
8. Repeat steps 3 through 7 to create the Distribution Directory Access rule for any additional distribution directory nodes or groups.

### ***Procedure:*** How to Test the Assignment of a Distribution Directory Access Rule to a Workspace

1. Sign in with the user ID and password of a member of the group to which the Distribution Directory Access role was assigned.
2. Right-click a report in the workspace, point to *Schedule*, and then click *Repository* to open the ReportCaster Distribution Scheduler wizard.
3. Click *Folder Location* to open the Browse for Folder dialog box.
4. Expand the File System folder that appears at the top of the Choose the folder tree.
5. If a folder with the name of the distribution directory node appears under the File System folder, click *OK* and close the ReportCaster Distribution Scheduler wizard.
6. If the folder for the distribution directory node does not appear, click *Cancel*, close the ReportCaster Distribution Scheduler wizard, and perform the following steps:
  - a. Right-click the distribution directory node, point to *Security*, and click *Rules on this Resource* in order to determine if the Distribution Directory Access rule is assigned to the group under which you signed in, and if it was not, assign the rule to the group.
  - b. Ensure that the List role is assigned to the FILE subsystem folder for the EVERYONE group.

### ***Procedure:*** How to Edit a Distribution Directory Node

You can use the Edit command to change the values in an existing distribution directory node, or to create a new node modeled on an existing node.

If you save an existing distribution directory node without changing the name, you overwrite the existing node with the revised version. However, if you save an existing distribution directory node with a new name, you automatically create a new node, and leave the existing node with the old name intact. You do not overwrite the existing node.

If you need to replace an existing node with a new node, you must delete the existing node after creating the new node. For more information, see [How to Delete a Distribution Directory Node](#) on page 122.

**Note:** The Type field is available only when you create a new distribution directory node. Therefore, you cannot change the type assigned to an existing Distribution Directory node.

1. On the Administration Console Configuration tab, expand the *File System Distribution Directories* folder, right-click your selected distribution directory, and then click *Edit*.
2. If you must rename the distribution directory node, type a new name for the distribution directory node in the Name field.
3. If this distribution directory node must connect to a new network location, in the Path field, type the new path for the distribution directory to an existing network location, using one of the following formats.

For Windows:

*drive:\path*

For UNIX or Linux:

*/path*

For the Universal Naming Convention:

*\\server\path*

where:

*drive*

Is the letter that represents the drive to which the server is mapped.

*server*

Is the name of the server that hosts the directory to which scheduled reports for the node identified in the Name field are to be directed.

*path*

Is the name of the network path to the directory to which scheduled reports for the node identified in the Name field are to be directed.

For example:

☐ For Windows: W:\ReportOutput\Report01

☐ For UNIX or Linux: /ReportOutput/Report01

☐ If using the Universal Naming Convention: \\Server01\ReportOutput\Report01

4. If this distribution directory node must connect to a new FTP server, click the name of that FTP Server in the Server list.

5. If you did not change the Name, click Save.

or

If you changed the Name, click Save As.

6. If you receive a message warning you to enter all required information, click *OK*, type the required information, and save the profile as described in steps 2 and 3.
7. If you receive a message stating that the node was successfully saved, click *OK*.

The Network Location page closes.

If you did not change the name, the updated node appears under the Distribution Directories folder.

If you changed the name, the new and the existing node appear under the Distribution Directories folder. You must assign the Distribution to File System and the Distribution Directory Access rule to the new distribution directory node to make it available to the groups that will use it for scheduled report distributions.

If you need to delete the existing node, see [How to Delete a Distribution Directory Node](#) on page 122.

### **Procedure: How to Delete a Distribution Directory Node**

1. On the Administration Console Configuration tab, expand the *Distribution Directories* folder, and then right-click the distribution directory node you want to delete.
2. Click *Delete*.
3. When you receive a message asking if you are sure you want to delete the node, click Yes.

The deleted node no longer appears under the Distribution Directories folder.

## **Understanding Application Settings**

Application Settings determine the configuration and behavior of the WebFOCUS web application.

For more information about configuration files, see [TIBCO WebFOCUS Client Configuration Files](#) on page 511. For more information about individual Application Settings, see *Application Settings*.

**Procedure: How to View or Edit Application Settings**

1. In the Administration Console, on the Configuration tab, expand the *Application Settings* folder and select the category of settings you would like to view or edit.

The settings appear in the main configuration pane.

2. Make the desired changes and click Save.

**Managing Automatic Sign Outs**

Client sessions that remain idle risk exposing sensitive information and system resources to unauthorized use. In order to minimize the time that a client session remains idle, two settings, located on the BI Portals page of the Administration Console Configuration tab, limit the length of an idle session to 120 minutes, by default.

The Session Timeout (minutes) (IBI\_SESSION\_TIMEOUT) setting limits session idle time for users who signed in with a valid User ID. Similarly, the Public Session Timeout (minutes) (IBI\_PUBLIC\_SESSION\_TIMEOUT) setting limits session idle time for public users who signed in with an Anonymous User ID.

As a best practice, we recommend that administrators replace the default values in both of these settings with shortest time that accommodates their security needs and supports typical resource usage for the two different user types.

To warn users that their idle sessions are about to expire, the Enable Auto Sign-out (IBI\_AUTO\_SIGNOFF) setting and the Idle Timeout message duration (minutes) (IBI\_AUTO\_SIGNOFF\_MESSAGE\_DURATION) setting also appear on the BI Portals page. When the Enable Auto Sign-out check box is selected, a message stating that the current session will expire due to inactivity opens after a session has been idle for the number of minutes specified by the relevant Session Timeout (minutes) setting.

The message remains open and visible for the number of minutes specified in the Idle Timeout message duration (minutes) setting, which is two minutes, by default. If the message opens from the Home Page or the Security Center, it includes a countdown of the remaining time before sign-out. If the message opens from a portal, the countdown does not appear.

To continue their session, users can click *OK*. This action closes the message box and restores the session. A new session timeout countdown starts as soon as the restored session goes idle.

If users do not click *OK* before the scheduled timeout, the message box closes, and the session comes to an end.

For users assigned to a zone that uses form-based authentication or another authentication method that requires them to present credentials before opening a new session, the window displaying the Home Page refreshes and displays the Sign in page automatically after the session ends.

For users assigned to a zone that uses a Single Sign On pre-authentication method, the window displaying the Home Page refreshes and displays the sign-out page specified in the Custom logout target URL setting opens instead.

Typically, this is the default sign-out page that does not link users to the sign-in page. However, this setting can also contain the URL of the sign-out page established by a pre-authentication provider, which ends the Single Sign On product session for that provider.

If the Security Center is open, the window displaying it will also refresh and display the Sign in page. Any other windows, such as the Administration Console, that were open at the time of the session timeout remain open and unchanged. However, you will receive an Unexpected Behavior error message the first time you attempt to use them after the timeout. When you click *OK* to clear this message, the window automatically refreshes and displays the Sign in page. As a best practice, we recommend that you close all but one window before signing in to WebFOCUS for a new session.

When users sign in again, or restart their session with authentication from their third-party authentication provider, the default page or portal defined in the Redirect `/ibi_apps` to setting opens, enabling them to return to tasks that may have been interrupted by the session timeout.

## Understanding Custom Settings

The Custom Settings page allows you to customize your product installation by typing customized values for standard settings.

When you save updates to settings that you type into the Customized Setting text box, they are transferred to the `site.wfs` file, located at `drive:\ibi\WebFOCUS82\client\wfc\etc`. When you use this page to assign new values to settings, they override the default values assigned to them. These overrides are carried over as you upgrade to new versions.

After you save a custom setting, the text continues to display on this page. You can use comments to identify specific updates and additional information about them.

For an example of applying custom settings, see [Managed Reporting Internal Variables](#) on page 723.



**Procedure: How to Configure Custom Settings**

Only an administrator can configure settings on the Custom Settings page.

1. In the Administration Console, on the Configuration tab, click *Custom Settings*.
2. Under the final comment statement at the top of the Custom Settings text box, or the most recent custom setting entry, type the variables, settings, commands, or comments that comprise the custom settings.

Use the format required by the application or operating system that will execute the command.

To help track changes to custom settings, use comments to identify and separate individual changes.

3. To store your custom settings in an encrypted format, select the *Encrypt* check box.

**Note:** Even when you select this check box, settings continue to appear in an unencrypted format in the Custom Settings text box.

4. When your configuration is complete, click *Save*.
5. When you receive a confirmation message, click *OK*.
6. When the Custom Setting page clears, click *Custom Settings* under the Application Settings folder to see your updated comments, settings, or commands in the Custom Settings text box.

**Understanding NLS Settings**

You can use the Administration Console to configure National Language Support and enable the Dynamic Language Switch.

Separate message files exist for every national language supported by the product. If you want to customize the set of characters used in your report output, you must select the code page for every language you use.

**Procedure: How to Configure National Language Support**

1. In the Administration Console, on the Configuration tab, click *NLS Settings* to open the NLS Settings page.
2. Click the option for the operating system on which the Client resides.

The list adjusts to display the available code pages for the selected operating system.

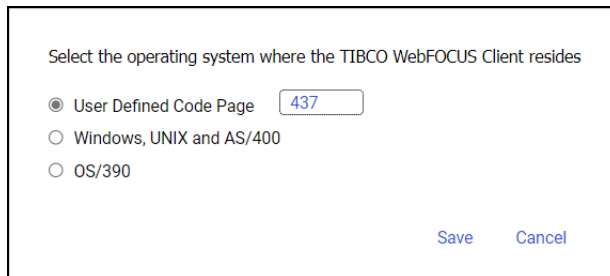
3. From the list, click a code page that configures the client for the correct display of report output in the browser.

**Note:** The language selected for the Client usually corresponds to the language selected for the Server from the Reporting Server Console.

If the language chosen from the Reporting Server Console does not appear in the drop-down list in the Administration Console, click *User Defined Code Page* and type the number of the user-defined code page.

Use this option, for example, when the server adds support for a new code page that is not yet reflected in the client software.

In the following sample configuration window, the administrator specified the *User Defined Code Page 437*.



Select the operating system where the TIBCO WebFOCUS Client resides

☒ User Defined Code Page

☐ Windows, UNIX and AS/400

☐ OS/390

Save Cancel

Unicode (UTF-8) is available for the Windows, UNIX, or AS/400 operating systems.

**Note:** Because of a Java encoding limitation for ISO8859-1, characters 0x80 through 0x9F are not supported with the Application Server configured for code page 137. As a result, French users wanting to display the following characters correctly should configure the Application Server to use Cp1252.

☐ U+0152 Latin Capital Ligature OE

☐ U+0153 Latin Small Ligature oe

4. Click Save to store your NLS settings. The console generates and updates the client configuration file (nlscfg.err), found in *drive:\ibi\WebFOCUS82\client\home\etc*, with the CODE\_PAGE setting. Note that if you click *NLS Settings* again, your new setting is highlighted as the active code page.

### **Reference:** Client Code Page Settings

The following code page settings are available:

☐ \* 137 - U.S. English/Western European

☐ 874 - Thai

☐ \* 942 - Japanese

☐ \* 946 - Simplified Chinese

- ☐ 949 - Korean
- ☐ 1250 - Eastern European
- ☐ 1251 - Russian
- ☐ \* 1252 - Western European
- ☐ 1253 - Greek
- ☐ 1254 - Turkish
- ☐ \* 1255 - Hebrew
- ☐ 1256 - Arabic
- ☐ 1257 - Baltic
- ☐ \* 10942 - Japanese EUC
- ☐ \* 10948 - Traditional Chinese
- ☐ \* 65001 - Unicode (UTF-8)

**Note:** Only those code page settings marked with an asterisk are fully supported in the current release.

## Customizing the Dynamic Language Switch

You can customize the languages that are made available on Sign in pages by activating the Dynamic Language Switch.

### **Procedure:** How to Customize the Dynamic Language Switch

1. In the Administration Console, on the Configuration tab, under the Application Settings folder, click *Dynamic Language Switch*.

The Dynamic Language Switch page opens with a list of the languages made available by the code page selection in the National Language Support page. By default, the Enable Dynamic Language check box is cleared and all of the language check boxes are deactivated.

The Dynamic Language Switch page also shows the Client Code Page setting specified in [How to Configure National Language Support](#) on page 125.

2. Select the *Enable Dynamic Language* check box to activate the check boxes for all of the available languages displayed in the panel, as shown in the following image.

To turn on the Dynamic Language Switch option on Sign in pages, click on the Enable Dynamic Language check box. The list of available languages to select from will be visible. Choose the languages you wish to enable in the Dynamic Language Switch box.

Client Code Page: 1252

☒ Enable Dynamic Language

<input type="checkbox"/>	Locale	Language Code	Locale Identifier string
<input checked="" type="checkbox"/>	English	en	en_US
<input type="checkbox"/>	English - Australian	au	en_AU
<input type="checkbox"/>	English - Canadian	ca	en_CA
<input type="checkbox"/>	English - United Kingdom	uk	en_GB
<input type="checkbox"/>	French - Canadian	fc	fr_CA
<input type="checkbox"/>	French - Standard	fr	fr_FR
<input type="checkbox"/>	German	de	de_DE
<input type="checkbox"/>	Indonesian	id	id_ID
<input type="checkbox"/>	Italian	it	it_IT
<input type="checkbox"/>	Portuguese - Brazilian	br	pt_BR
<input type="checkbox"/>	Spanish	es	es_ES
<input type="checkbox"/>	Spanish - Mexican	mx	es_MX

Save Cancel

3. Select the check box next to each of the languages that you want to appear on the Sign in pages and in the Language menu.
4. Select the check box next to the Locale heading if you want all of the languages to appear in the Select Languages drop-down list on the Sign in pages and in the Language menu.
5. Click Save.
6. When you receive a message stating that your change was saved successfully, click OK.

**Note:** To remove languages from the Select Languages list on the Sign in pages, clear the check boxes next to the languages you want to remove.

## Understanding Redirection Settings

Redirection settings specify the way in which the Client handles output files by file extension. You can review these settings through the Redirection Settings page of the Administration Console Configuration tab. Each entry in the page identifies an output file format by its TIBCO WebFOCUS Extension, Content Type, File Format, Server Extension, Client Extension, and IBFS File Format, as shown in the following image.

Redirection Settings

WebFOCUS Extension	Content Type	Format	Redirect	Server Extension	Save Report	Client Extension	IBFS Format
.wp	text/plain	ascii	no	N/A	no	.wp	ascii
.xht	application/vnd.ms-excel	ascii	no	XHT	yes	.xls	ascii
.xls	application/vnd.ms-excel	binary	yes	EXCEL	no	.xls	binary
.xism	application/vnd.ms-excel.sheet.macroEnabled.12	binary	no	XLISM	yes	.xism	binary
.xlsx	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	binary	no	XLTX	yes	.xlsx	binary
.xltn	application/vnd.ms-excel.template.macroEnabled.12	binary	no	XLTM	yes	.xltn	binary
.xltx	application/vnd.openxmlformats-officedocument.spreadsheetml.template	binary	no	XLTX	yes	.xltx	binary
.xmh	application/vnd.ms-excel	ascii	no	XMH	yes	.xls	ascii
.xml	text/xml	ascii	no	XML	no	.xml	binary
.zip	application/zip	binary	no	ZIP	yes	.zip	binary

Save Cancel ☐ Encrypt

**Note:** This image displays the lower half of the page to show file extensions with varying values in the Redirect and Save Report fields.

The mime.wfs file, located in the directory `drive:\ibi\WebFOCUS82\client\wfc\etc`, contains information about available format types. When you open the Redirection Settings page, you display redirection settings stored in the mime.wfs file, and when you save changes, you store them in the mime.wfs file.

Before making any changes to the redirection settings, you must assess the impact they will have on the applications and user experience within your organization. If you require further assistance, consult Customer Support Services.

### Notes:

- ☐ For more information about the Redirection (IBIWF\_Redirect) configuration tab setting that appears on the Client Settings page, see *Client Settings*.
- ☐ When the Resource Governor Advise Messages (IBI\_RES\_GOV\_ADVISE) setting, located on the Client Settings page of the Administration Console Configuration tab, is enabled for a selected Reporting Server, redirection is turned on for all report formats when the server returns any Resource Governor advise messages to display to the user. For more information, see the Resource Governor Advise Messages (IBI\_RES\_GOV\_ADVISE) setting definition in *Client Settings*.

## Redirecting and Saving File Output

On the Redirection Settings page, values in the Redirect and Save Report settings determine whether the output from a request is stored in a temp folder file during processing, and whether a name is to be assigned to that file automatically. The combination of values assigned to these two settings determines the way in which output from requests is to be displayed and saved.

The Redirect setting allows you to specify if the output from a request should be saved to a file in the temp folder located under the client directory.

- ☐ If the value in the Redirect setting is yes, the output is saved to a file in the temp folder, where a name can be assigned to it, as directed by the value assigned to the Save Report setting.
- ☐ If the value in the Redirect setting is len, the output is saved to a file in the temp folder only if it exceeds the value assigned to the IBIWF\_sendbufsize setting, which, by default, is 16384 bytes. Any output that must be saved to a file in the temp folder is then sent to the browser without an additional HTTP call.
- ☐ If the value in the Redirect setting is no, output is processed as directed by the value assigned to the Save Report setting.

The Save Report setting allows you to specify if report files should be assigned names automatically when they are created.

- ☐ If the value in the Save Report setting is no, the report, chart, or other output opens directly in the Browser or application without prompting users to open or save it. Users still have the option to save the report after it is opened. A randomly-generated name is assigned to the report output file regardless of whether the request originated from the Resources tree, or from InfoAssist, WebFOCUS® App Studio, or some other application tool.
- ☐ If the value in the Save Report setting is yes, the report, chart, or other output is saved to a file in the temp folder, as follows:
  - ☐ If the report request specifies an output file name, it is assigned to the output file. Then the browser makes an HTTP call to retrieve the temporary stored output file, and prompts the user to open, save, or cancel it.
  - ☐ Reports, charts, or other content files that require a date and time can be created by including the following coding technique that uses amper variables to specify the filename and capture the date and time the report is created by the Reporting Server. For more information, see the example in the topic, [Adding a Date and Time to the PCHOLD AS Filename](#) on page 132.

- ☐ If the report request does not specify a file name:
  - ☐ If you run the report from an item in the Resources tree, the name value of that item is assigned to the request output file, and the date and time that the file was created is automatically added to the file name.
 

**Note:** The name value of an item appears on the Properties panel in the Name field.
  - ☐ However, if the *Do Not Assign Timestamp to a Redirected Report Name* setting check box is also selected, the automatic date and time assignment is not added to the file name.
  - ☐ If you run the report from a tool, such as TIBCO WebFOCUS Designer, InfoAssist, the Text Editor, or the App Studio Report Canvas, a randomly-generated name is assigned to the output file, and the date and time that the file was created is automatically added to the file name.
  - ☐ However, if the *Do Not Assign Timestamp to a Redirected Report Name* setting check box is also selected, the automatic date and time assignment is not added to the file name.

### Specifying an Output File Name Within a Report Request

To specify an output file name within a report request, use the PCHOLD AS *filename* option.

Within a report request, the syntax for the PCHOLD option is:

```
ON TABLE PCHOLD [AS filename] [FORMAT fmt]
```

where:

**AS filename**

Specifies a name for the PCHOLD file.

**FORMAT fmt**

Specifies the format of the PCHOLD file. For example, XLSX.

**Note:** If the PCHOLD AS name specified in the report request contains eight or fewer characters, it is returned to the browser in uppercase. If it contains nine or more characters, it is returned to the browser in the case specified.

For information on creating reports with the PCHOLD command, see the *Creating Reports with TIBCO WebFOCUS Language* guide.

## Adding a Date and Time to the PCHOLD AS Filename

Some applications, such as Microsoft Excel®, require a unique name for every file opened. In order to accommodate this requirement, when you assign a value of yes to the Save Report setting, you can add amper variables to the report request to obtain the date and time the report is created by the Reporting Server, specify a file name with the date and time appended, and assign that file name to the report file, as shown in the following example:

```
-SET &TIME = STRIP(8,&TOD,',' ,A8);
-SET &FNAME = OUTPUT_ | &YYMD | _ | &TIME;
TABLE FILE CAR
BY CAR
ON TABLE PCHOLD AS &FNAME FORMAT XLSX
END
XSLX
```

### Procedure: How to Change Redirection Settings

Before making any changes to the Redirection Settings, you must assess the impact they will have on the applications and user experience within your organization. You may need to consult with the administrators of other large scale applications or network administrators within your organization that would be affected by your changes. If you require further assistance, consult Customer Support Services.

1. In the Administration Console, on the Configuration tab, click *Redirection Settings*.
2. In the Redirect list:
  - a. Click *yes* to redirect the output to a temporary directory for files using the specified extension.
  - b. Click *no* to allow the output to be processed as directed by the value assigned to the Save Report setting.
  - c. Click *len* to redirect report content to a temporary directory only when it exceeds the buffer size defined in the IBIWF\_sendbufsize setting.
3. In the Save Report list:
  - a. Click *yes* to prompt users in the browser to open or save the output for files using the specified extension.
  - b. Click *no* to open output directly in the Browser or application without prompting users to open or save it.
4. If you want to encrypt the redirection settings, select the *Encrypt* check box at the bottom of the screen.
5. Click *Save* to save your changes in the Redirection Settings panel.



## Saving GRAPH (PNG, SVG, GIF, JPEG, or JPG) Requests

In order to use the Save Report functionality for GRAPH requests that specify a PNG, SVG, GIF, JPEG, or JPG format in the procedure, you must take the following steps:

1. Set Save Report to yes for the .htm extension.

Running a server-side GRAPH request creates an HTM file that contains a link to the actual graph output, which is stored as a temporary image file with a .jpeg, .jpg, .gif, .svg, or .png extension.

2. When you execute a GRAPH request, if you select the Save option when prompted to open or save the output, the output is saved to an HTM file using only a reference to the graph image, which will eventually expire and be deleted from the server, as determined by the temporary file expiration settings in the Client Configuration.
3. To preserve the output of the GRAPH request, open the saved HTM file, right-click the graph image, and select *Save Picture As* to save it to disk permanently. You can then substitute an absolute reference to the saved image file in the HTM output file.

## Understanding InfoAssist Properties

InfoAssist Properties allow you to set the system-wide defaults that apply to all InfoAssist users. To update these settings, select the *Configuration* tab, and then select *InfoAssist Properties*. For more information about specific InfoAssist Properties see [InfoAssist Properties](#) on page 575.

## Understanding TIBCO WebFOCUS Designer Properties

WebFOCUS Designer Properties allow you to set the system-wide defaults that apply to all users of WebFOCUS Designer. To update these settings, select the *Configuration* tab, and then select *Designer Properties*. For more information about specific WebFOCUS Designer Properties, see [TIBCO WebFOCUS Designer Properties](#) on page 574.

## Understanding the Role Update Utility

The Role Update Utility lists the differences between the privileges currently assigned to Repository Roles and their corresponding Package Roles. Repository Roles are defined in the repository, and are used by resource templates. Package Roles are maintained in a separate file, and define the standard set of privileges assigned to roles within a release.

When you upgrade to a new release, or change the privileges assigned to Repository Roles by updating them in the Security Center, this utility identifies all variances between the privileges assigned to the Repository Roles used by resource templates and the standard set of privileges defined by the Package Role.

For each Repository Role whose set of assigned privileges varies from its corresponding Package Role, the utility gives you the option to disregard the variance, add the missing privileges to the Repository Role, or replace the Repository Role entirely with the standard set of privileges defined in the Package Role. Replacing a Repository Role with a Package Role is the only way to remove any additional privileges that appear in a Repository Role but not in the corresponding Package Role. The utility also enables you to make these changes globally to all Repository Roles whose set of assigned privileges vary from the set of privileges assigned to the Package Roles.

After an upgrade or installation of a new release, the utility enables you to identify all variances between the existing Repository Roles and the new Package Roles and incorporate the new privileges into the Repository Roles or maintain them without updates.

If there are no upgrades or changes, a role entry displays the message, No privilege differences between package and repository. If this is the case with your display, you can disregard this feature until you upgrade or change a Repository Role.





For more information on how to update a role after a typical installation, see the *TIBCO WebFOCUS and ReportCaster Installation and Configuration* technical content.

Working With HTML5 Chart Extensions

The HTML5 Chart Extensions page contains all currently installed HTML5 chart extensions, as shown in the following image.

HTML5 Chart Extensions

Get more Extensions


 com.ibi.arc	<div><div>Name: Arc Chart</div><div>Description: Arc Chart</div><div>Version: 1.2.0</div><div>API Version: 2.0</div><div>Author: Three D Graphics</div><div>Copyright: Three D Graphics Inc.</div><div>URL: <a href="https://threedgraphics.com">https://threedgraphics.com</a></div><div>License:</div></div>	<div><input checked="" type="checkbox"/> Enabled</div> <div>✖</div>
 com.ibi.calendar	<div><div>Name: Calendar Heat Map Chart</div><div>Description: Heat Map chart that has weekdays on one axis and months on the other.</div><div>Version: 1.3</div><div>API Version: 1.0</div><div>Author: TIBCO Software</div><div>Copyright: TIBCO Software Inc.</div><div>URL: <a href="https://github.com/ibi/vf-extensions-chart/tree/master/com.ibi.calendar">https://github.com/ibi/vf-extensions-chart/tree/master/com.ibi.calendar</a></div><div>License:</div></div>	<div><input checked="" type="checkbox"/> Enabled</div> <div>✖</div>
 com.ibi.calendar_traditional	<div><div>Name: calendar_traditional</div><div>Description: Traditional Calendar</div><div>Version: 1.0</div><div>API Version: 1.0/2.0</div><div>Author: TIBCO Software</div><div>Copyright: TIBCO Software Inc.</div><div>URL: <a href="https://github.com/ibi/vf-extensions-chart/tree/master/calendar_traditional">https://github.com/ibi/vf-extensions-chart/tree/master/calendar_traditional</a></div><div>License:</div></div>	<div><input type="checkbox"/> Enable</div> <div>✖</div>
 com.ibi.cartogram	<div><div>Name: USA State Cartogram</div><div>Description: Cartogram for U.S. States</div><div>Version: 1.1.0</div><div>API Version: 1.0</div><div>Author: TIBCO Software</div><div>Copyright: TIBCO Software Inc.</div><div>URL:</div><div>License:</div></div>	<div><input type="checkbox"/> Enable</div> <div>✖</div>

HTML5 chart extensions expand the standard set of charts to include customized charts tailored to very specific reporting and data visualization requirements. For more information about Chart Extensions, see the *Installing a Chart Extension* topic in the *Creating HTML5 Charts With WebFOCUS Language* manual.

Features on this page allow you to upload HTML5 chart extensions, enable or disable their use, and uninstall them when no longer needed.

## Understanding HTML5 Chart Extension Entries

Each HTML5 Chart Extension entry contains details that identify a chart extension and its origin, and help you determine if a chart extension is appropriate.

  
com.ibi.chord


Name: Chord Diagram  
Description: Chord Diagram  
Version: 1.6  
API Version: 1.0  
Author: Three D Graphics  
Copyright: Three D Graphics Inc.  
URL: <https://github.com/ibi/vf-extensions-chart/tree/master/com.ibi.chord>  
License: BSD 3-clause

Each entry identifies an HTML5 chart extension with a Name, Description, Version, and API Version. These details help you identify the chart extension you want to use, and the specific version of it that best matches your requirements. The Author and Copyright identify the origin of the chart extension, and the URL links you to the location where you can retrieve additional copies. License information identifies the type of license, if any, under which the chart extension is made available to you, and helps you understand any limits on the use of the chart extension and the rights and obligations licensed users have to the developer.


## Understanding the HTML5 Chart Extensions Enable/Enabled Check Box

Every HTML5 Chart Extension entry includes the Enable/Enabled check box that indicates whether or not the chart extension is available for use. The use of this check box provides administrators with a second level of availability that enables them to restrict the full availability of HTML5 Chart Extensions to those that are in active use, while retaining all other installed HTML5 Chart Extensions in readiness for when they are needed.

When this check box is cleared, it displays the Enable label to indicate that selecting the check box will make the chart extension available for use, as shown in the following image.

  
com.ibi.chord

Name: Chord Diagram  
Description: Chord Diagram  
Version: 1.6  
API Version: 1.0  
Author: Three D Graphics  
Copyright: Three D Graphics Inc.  
URL: <https://github.com/ibi/vf-extensions-chart/tree/master/com.ibi.chord>  
License: BSD 3-clause

☐ Enable 

HTML5 Chart Extensions that have the Enable check box selected are installed, but they are not available to users.

When this check box is selected, it displays the Enabled label to indicate that the chart is already available for use, as shown in the following image.

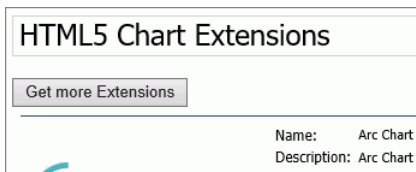


HTML5 Chart Extensions that have the Enabled check box selected are installed and are available to developers using InfoAssist for their use in chart creation. The files and directories included in that Chart Extension are identified as eligible for calls from InfoAssist and Designer. An icon for that Chart Extension is displayed in the Select a Chart menu that opens from the Other command in the Chart Type group, on the InfoAssist Format tab ribbon.

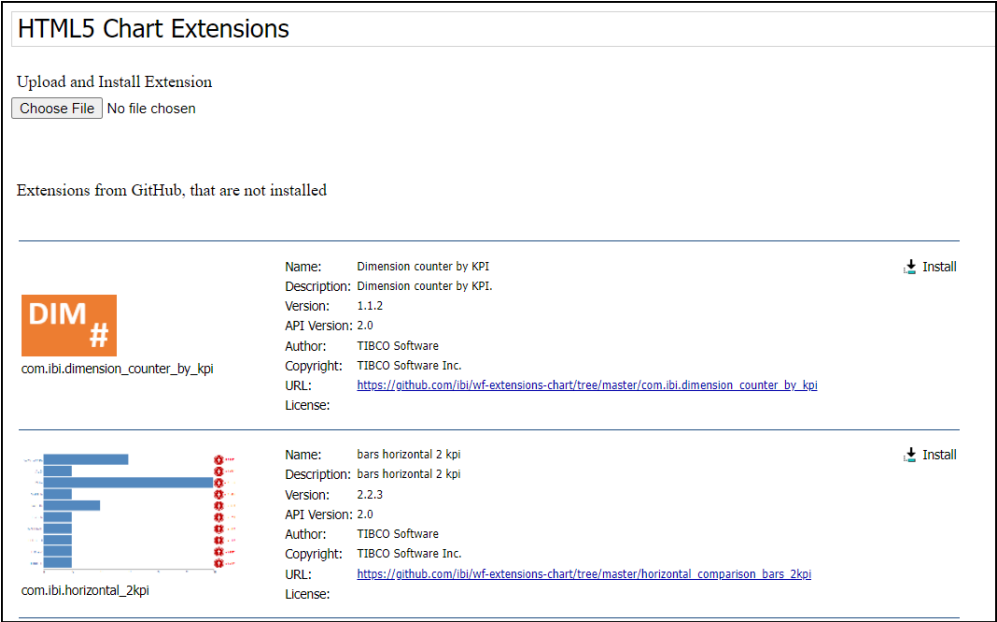
**Note:** The HTML5 Chart Extensions page does not manage copyright or license restrictions. You are ultimately responsible for the use of any HTML 5 Chart Extension you upload. Therefore, you must ensure that you have a license or permission to use any HTML5 Chart Extension before uploading it to this page.

## Uploading Additional HTML5 Chart Extensions Using the Upload and Install Extensions Page



Use the Upload and Install Extensions page to install additional HTML5 Chart Extensions. To open the Upload and Install Extensions page from the main HTML5 Chart Extensions page, click *Get more Extensions*, as shown in the following image.



The Upload and Install Extensions page opens, as shown in the following image.



The Upload and Install Extensions page provides two ways to install additional HTML5 Chart Extensions:

- ❑ By clicking the *Install Extension* button  in entries for chart extensions that are found on the Information Builders public extension GitHub page, <https://github.com/ibi/wf-extensions-chart>, but are not currently installed.
- ❑ By clicking the *Choose File* button  next to Upload and Install Extension field to navigate to a folder on your local file system that contains a locally-developed HTML5 Chart Extension package in .zip file format.

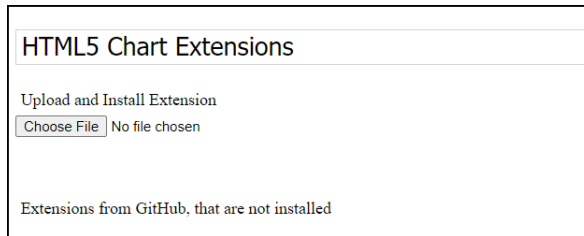
To move back to the main HTML5 Chart Extensions page from the Upload an Install Extensions page, click *HTML Chart Extensions* under the Application Settings Folder, or click the *Back* button in your browser.

**Procedure: How to Upload HTML5 Chart Extensions from the Local File System**

Use this procedure to upload zip files containing HTML5 Chart Extensions from your local system.

You must ensure that you have a license or permission to use any HTML5 Chart Extension before uploading it to this page.

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, click *HTML5 Chart Extensions*.
3. On the HTML5 Chart Extensions page, click *Get more Extensions*.
4. On the Upload and Install Extension page, click *Choose File*, as shown in the following image.



The Open dialog box opens and points to the extensions folder for your local installation. Typically, this is the following folder:

`drive:\ibi\install_dir\config\web_resource\extensions`

where:

`install_dir`

Is your TIBCO WebFOCUS installation directory.

**Note:** If you downloaded your HTML5 Chart extension zip file to a different directory, navigate to that directory and file.

5. Click the file containing the zipped version of the HTML5 Chart extension you want to upload, and then click *Open*.
6. When the HTML5 Chart Extensions page refreshes and returns you to the top, scroll down to the entry for the new HTML5 Chart Extension.


**Note:** For more information about creating your own HTML5 Chart Extensions, see the *Creating a Chart Extension* topic in the *Creating HTML5 Charts With WebFOCUS Language* manual.

### **Procedure:** How to Install HTML5 Chart Extensions From the IBI GitHub Page

Use this procedure to upload HTML5 Chart Extensions from the public IBI GitHub extension page, <https://github.com/ibi/wf-extensions-chart>.

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, click *HTML5 Chart Extensions*.
3. On the HTML5 Chart Extensions page, click *Get more Extensions*.
4. On the Upload and Install Extension page, review the list of extensions from GitHub that are not installed, as shown in the following image.



5. If the chart extension you want to install appears in the list, click *Install Extension* .
6. When the HTML5 Chart Extensions page refreshes and returns you to the top, scroll back to your entry to confirm that the chart extension is now installed.

### **Procedure:** How to Enable an Installed HTML5 Chart Extension

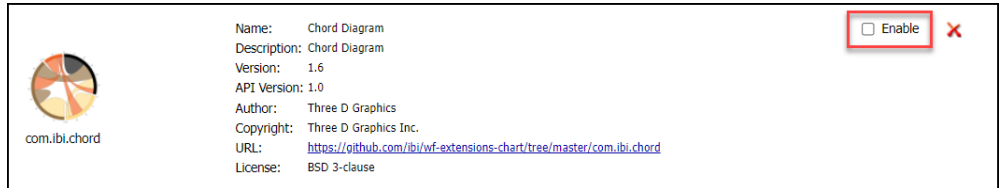
When you select the Enable check box in an HTML5 Chart Extension entry, you make it available for use. You must ensure that you have a license or permission to use any HTML5 Chart Extension before making it available.

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, click *HTML5 Chart Extensions*.
3. On the HTML5 Chart Extensions page, scroll to the entry for the HTML5 Chart Extension that you want to enable.

**Note:** You can also search for the chart extension by name, using the Find or Find on this page command that is supported by the browser.



4. Select the *Enable* check box, as shown in the following image.



5. When the HTML5 Chart Extensions page refreshes and returns you to the top, scroll back to your entry to confirm that the check box is now selected.

An icon for the HTML5 Chart Extension appears in the InfoAssist Select a Chart menu, which opens when you click the Other command in the Chart Types group on the Format tab, and in the Custom section of the Content Picker, which opens from the right side of the Designer canvas.

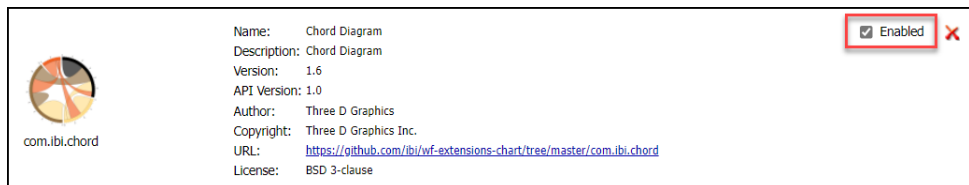
### **Procedure:** How to Disable an HTML5 Chart Extension

When you clear the Enabled check box in an HTML5 Chart Extension entry, you make it unavailable for use. However, the chart extension remains installed on the HTML5 Chart Extension page and can be enabled again when needed.

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, click *HTML5 Chart Extensions*.
3. On the HTML5 Chart Extensions page, scroll to the entry for the HTML5 Chart Extension that you want to make unavailable.

**Note:** You can also search for the chart extension by name, using the Find or Find on this page command that is supported by the browser.

4. Clear the *Enabled* check box, as shown in the following image.



5. When the HTML5 Chart Extensions page refreshes and returns you to the top, scroll back to your entry to confirm that the check box is now cleared.

The icon for the HTML5 Chart Extension no longer appears in the Select a Chart Menu that opens from the InfoAssist ribbon, or in the Custom section of the Content Picker, which opens from the right side of the Designer canvas.

### **Procedure:** How to Uninstall an HTML5 Chart Extension

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, click *HTML5 Chart Extensions*.
3. On the HTML5 Chart Extensions page, scroll to the entry for the HTML5 Chart Extension that you want to uninstall.

**Note:** You can also search for the chart extension by name, using the Find or Find on this page command that is supported by the browser.

4. Click *Delete\_CHARTNAME\_Chart*, represented by the red X icon, as shown in the following image.



5. When you receive a message asking if you want to permanently delete the extension, click Yes.
6. When the HTML5 Chart Extensions page refreshes and returns you to the top, scroll back to your entry to confirm that the entry is now deleted.

The entry for the HTML5 Chart Extension no longer appears on the page. If the HTML5 Chart Extension was installed from the GitHub page, it now appears on the Upload and Install Extensions page and can be reinstalled from that page. If it was installed from your local file system, it does not appear on that page, and you will be required to use the Upload and Install Extension field and Browse button to reload the chart extension from your local file system.

## Configuring TIBCO WebFOCUS Security

In the Administration Console, you configure the security settings that govern authentication and authorization in your environment.

Security can either be configured internally in the Repository, or externally in a directory that is not part of TIBCO WebFOCUS. To configure settings for internal security, use the settings in the Internal page. To configure a connection to an external directory that is not part of TIBCO WebFOCUS, such as Microsoft Active Directory or LDAP Directory, use the External page.

## Understanding Internal Security Page Settings

Internal authentication and authorization are enabled, by default. Optionally, you can use the settings in the Internal page to configure sign in and password policies.

### **Sign In Settings (Enable Sign In Settings)**

Determines the default values assigned to the Sign In Settings on the Internal Security Page.

This check box is cleared (False), by default. Sign In Settings are inactive and unavailable and display a value of 0.

When this check box is selected (True), Sign In Settings are activated, automatically assigned a set of pre-configured values, and made available for updates. To deactivate an individual setting while this check box is selected, type or select zero (0). When this check box is later cleared, all values assigned to the Sign In Settings return to 0, and the settings are deactivated.

This setting does not affect the value or availability of the Password Expiration Result options.

### **Maximum Sign-in Attempts (IBI\_Max\_Bad\_Attempts)**

Specifies the number of unsuccessful sign-in attempts allowed before the account status is changed to locked. When the Sign In Settings check box is cleared, the default value is 0, which allows unlimited attempts. When the Sign In Settings check box is selected, the default value is 5, and administrators can type or select an alternative value. To deactivate this setting when the Sign In Settings check box is selected, type or select 0.

### **Lockout Duration (Minutes) (IBI\_Account\_Lockout\_Duration)**

Specifies the number of minutes before the status of an account changes from locked to active. When the Sign in Settings check box is cleared, the default value is 0 (off). When the Sign In Settings check box is selected, the default value is 3 minutes, and administrators can type or select an alternative value. To deactivate this setting when the Sign In Settings check box is selected, type or select 0.

**Lockout Duration Reset (Minutes) (IBI\_Account\_Lockout\_Duration\_Reset)**

Specifies the number of minutes that must elapse after the number of failed sign-in attempts specified by the Maximum Sign in Attempts setting before the allowed sign-in attempt counter is reset to 0. The available range is from 1 to 99,999 minutes. When the Sign In Settings check box is cleared, the default value is 0 (off). When the Sign In Settings check box is selected, the default value is 3 minutes, and administrators can type or select an alternative value. To deactivate this setting when the Sign In Settings check box is selected, type or select 0.

**Days Until Password Expires (IBI\_Password\_Expire)**

Specifies the number of days that a password will remain active. When the Sign In Settings check box is cleared, the default value is 0, which prevents passwords from expiring. When the Sign In Settings check box is selected, the default value is 90 days. Once the password has expired, the user must take the action specified by the Password Expiration Result (IBI\_Password\_Expire\_Action) setting, and administrators can type or select an alternative value. To deactivate this setting when the Sign In Settings check box is selected, type or select 0.

**Days Until Password Expiration Warning (IBI\_Password\_Expire\_Warning)**

Specifies the number of days prior to expiration that a warning will be displayed to the user. When the Sign In Settings check box is cleared, the default value is 0, which provides no warning. When the Sign In Settings check box is selected, the default value is 75 days. This value should be less than or equal to the value assigned to the Days Until Password Expires (IBI\_Password\_Expire) setting, and administrators can type or select an alternative value. To deactivate this setting when the Sign In Settings check box is selected, type or select 0.

**Password Expiration Result (IBI\_Password\_Expire\_Action)**

Specifies the action required when a password expires. You can choose one of the following options:

- ☐ *To force users with expired passwords to change their passwords before signing in. (MUSTCHANGE) This is the default value.*
- ☐ *Change the status of users with expired passwords to inactive. Such users cannot sign in until an administrator resets the password. (DISABLE-USER)*

**Enable Password Complexity (IBI\_Password\_Complexity)**

Determines the default values assigned to the Password Settings on the Internal Security Page.

This check box is cleared (False), by default. All of the Password Settings are inactive and unavailable and display a value of 0.

When this check box is selected (True), all of the Password Settings are activated and available for updates. WebFOCUS automatically assigns a pre-configured set of values to them.

When this check box is later cleared, all values assigned to the Password Settings return to 0, and the settings are deactivated.

If this check box is selected (True), passwords also must:

- ☐ Not contain the user account name or parts of the full name of the user that exceed five consecutive characters.
- ☐ Be at least six characters long or at least the number of characters specified in Minimum Password Length, whichever is greater.
- ☐ Contain characters from three of the following four categories:
  - ☐ Uppercase English characters (A through Z).
  - ☐ Lowercase English characters (a through z).
  - ☐ Base 10 digits (0 through 9).
  - ☐ Non-alphabetical characters (for example, !, \$, #, %).
- ☐ Complexity requirements are enforced when passwords are changed or created.

#### **Minimum Password Length (IBI\_Password\_Minimum\_Length)**

Defines the required minimum length of a password. When the Enable Password Complexity check box is cleared, the default value is 0 characters. When the Enable Password Complexity check box is selected, the default value is 6 characters. To deactivate this setting when the Enable Password Complexity check box is selected, type or select 0.

#### **Password Reuse (IBI\_Password\_Reuse)**

Specifies the number of recent passwords that cannot be reused. If Password Reuse is set to 6, for example, the 6 most recent password changes are tracked, and you are prevented from reusing them when creating a new password. When the Enable Password Complexity check box is cleared, the default value is 0 changes, and users can re-use any previously-assigned password. When the Enable Password Complexity check box is selected, the default value is 2 changes. To deactivate this setting when the Enable Password Complexity check box is selected, type or select 0.

**Procedure: How to Configure Sign In Settings**

1. In the Administration Console, click the *Security* tab.
2. On the Security page, under the Security Configuration folder, click *Internal*.
3. Select the *Sign In Settings* check box.

The Internal page displays the following default values:

- ☐ Maximum Sign-in Attempts – 5
  - ☐ Lockout Duration (Minutes) – 3
  - ☐ Lockout Duration Reset (Minutes) – 3
  - ☐ Days Until Password Expires – 90
  - ☐ Days Until Password Expiration Warning – 75
4. To change the default value assigned to any of these settings, type or select an alternate value in any of these boxes.
  5. To clear all settings, clear the *Sign In Settings* check box. All values automatically return to 0.
  6. In the Password Expiration Result section, accept the default option *To force users with expired passwords to change their passwords before signing in*, or click the alternative option *Change the status of users with expired passwords to inactive. Such users cannot sign in until an administrator resets the password*.
  7. Continue with any other Internal Security page updates or save your changes.

**Procedure: How to Configure Password Settings**

1. In the Administration Console, click the *Security* tab.
2. On the Security page, under the Security Configuration folder, click *Internal*.
3. Select the *Enable Password Complexity* check box.

The Internal page displays the following default values:

- ☐ Minimum Password Length – 6
  - ☐ Password Reuse - 2
4. To change the default value assigned to any of these settings, type or select an alternate value in either of these boxes.
  5. To clear all settings, clear the Password Settings check box. All values automatically return to 0.

6. Continue with any other Internal Security page updates or save your changes.

**Procedure: How to Save Internal Security Page Configuration Updates**

1. When all of your Internal Security Page Configuration updates are complete, click *Save*.
2. When you receive a confirmation message, click *OK*.
3. When you receive a message to clear the cache, click *OK*.
4. In the Administration Console menu bar, click *Clear Cache* and, when you receive a confirmation message, click *OK*.

## Understanding External Security Page Settings

Use the External page if you configure security in a directory that is not part of TIBCO WebFOCUS.

### Enable External Security

When you select this check box, internal security settings are overridden and all authentication activities and approvals are directed to the external system you identify on this page. Fields and features in the section below this check box become available and respond to updates from Administrators.

### External Security Type (IBI\_Authentication\_Type)

The list box for this field contains the following values:

- ☐ **Reporting Server.** Definition is currently unavailable.
- ☐ **Legacy LDAP.** Authenticates users against an AD or LDAP directory. Do not select this option unless advised to do so by the Customer Support Team.
- ☐ **Custom Java Plug-In.** Definition is currently unavailable. Do not select this option unless advised to do so by the Customer Support Team.

### Reporting Server Node

Specifies the name of the Reporting Server that manages communications with the external authentication provider application.

### Server Administrator ID

Specifies the ID of the administrator of the external security server. To make the User Authorization section available, you must type the ID of a valid user that is already defined on the external security server in this field. Typically this is the user ID you assign to the server manager during the installation.

### Password

Specifies the Password assigned to the administrator of the external security server. To validate the ID and password of the external Server administrator, click *Connect*. When you submit a valid ID and password, the User Authorization section becomes available.

### User Authorization

The location where authorization is granted to users. The options and check boxes in this section become available only after you type a valid user ID in the Server Admin ID field and click *Connect*.

- ☐ **Internal.** TIBCO WebFOCUS manages all user authorization tasks.
- ☐ **Internal and External.** TIBCO WebFOCUS and the external application share the management of authorization tasks.
- ☐ **External Only.** The external application manages authorization tasks.
- ☐ **Group Provider Override.** When selected, this check box and the field associated with it identify the external provider that overrides group authorization.

**Note:** This check box appears only after you click the options Internal and External, or External Only, the Group provider Override checkbooks and field appear.

### Account Creation on Sign In

Specifies the range of user accounts that will be created upon their first sign-in attempt.

- ☐ **All.** Specifies the creation of an account for all users upon their first sign-in attempt.
- ☐ **Mapped External Groups.** Specifies the creation of an account only for those users in Mapped External Groups upon their first sign-in attempt.
- ☐ **Off.** Disables the automatic creation of user accounts.

### Synchronize User Information

Activates the automatic retrieval of user information for the Description and EMail Address fields when users sign in to TIBCO WebFOCUS, helping to ensure that the most current user information is always available.

If this check box is cleared, the default setting, the Description and EMail Address fields of a user are not updated when that user signs in.



If this check box is selected, the Description and EMail Address fields of a user are updated when that user signs in. The source of this information depends upon the selection of one of the following options:

- ☐ **With Authentication Provider.** If this option is selected, updated Description and EMail Address field information is received from the *authentication* provider. This option is selected, by default.
- ☐ **With Authorization Provider.** If this option is selected, updated Description and EMail Address field information is received from the *authorization* provider.

The values assigned to this setting apply equally to users who sign in to a security zone using Form Based authentication as well as Pre-authentication, as long as External Security is in use.

## Using Advanced Settings

The Advanced page in the Security tab of the Administration Console provides access to settings that identify specialized administrative user IDs and passwords and additional security features that apply to the entire WebFOCUS installation.

Settings on the Advanced page identify the ID of the Anonymous User, which is invoked when users select the Public Access link from the sign-in screen. Settings on this page also identify the ID and password of the Root User, who is the Superuser that maintains unlimited access to WebFOCUS. The Root User serves as a fallback when all other users are locked out or whenever a user with all-access permissions is required to maintain system operations.

### Multiple Sign-ins Per User (IBI\_MULTIPLE\_LOGINS\_PER\_USER)

Specifies whether the same user can have multiple sign-ins, which are authenticated sessions, open simultaneously. When this check box is selected, (True), a user can have multiple authenticated sessions open simultaneously. When it is cleared, (False), a user can have only one authenticated session open at a time.

The ability to maintain multiple open authenticated sessions per user is available only in the Enterprise Edition of WebFOCUS. Other editions allow only one open authenticated session per user.

- ☐ In the Enterprise Edition, this check box is selected (True), by default.
- ☐ In all other editions, this check box is cleared (False), by default, and is unavailable.

**Root User (IBI\_ADMIN\_NAME)**

Specifies the user ID of the administrator or superuser. When Root User (IBI\_Admin\_Name) and Root Password (IBI\_Admin\_Pass) are set, this user is given ALL permissions, regardless of other policies set within the system. Typically, this user ID is used under limited circumstances and removed when no longer needed.

**Root Password (IBI\_ADMIN\_PASS)**

Specifies the password of the administrator or superuser.

**Reporting Server Anonymous User ID (IBI\_ANONYMOUS\_WFRS\_USER)**

Specifies the user ID that the WebFOCUS Client uses to connect to the Reporting Server for anonymous, or unauthenticated, requests. Used when you sign in as a Public User. For more information on configuring the Reporting Server, see [TIBCO WebFOCUS Reporting Server Settings](#) on page 88.

**Reporting Server Anonymous Password (IBI\_ANONYMOUS\_WFRS\_PASS)**

Contains the password used by the anonymous user for connections to the Reporting Server. This applies to all authentication types. Used when you sign in as a Public User.

**Anonymous User ID (IBI\_ANONYMOUS\_USER)**

Specifies the user ID that the WebFOCUS Client uses for unauthenticated requests. By default, the value is *public*.

By default, the WebFOCUS Client supports anonymous, or unauthenticated, access to resources made available to users in the Anonymous group, as well as to procedures on the WebFOCUS Reporting Server. The Reporting Server credentials used by this setting are specified by Reporting Server Anonymous User ID (IBI\_WFRS\_Anonymous\_User) and Reporting Server Anonymous Password (IBI\_WFRS\_Anonymous\_Pass).

**Note:** This setting is relevant only to the Enterprise Edition, which is the only edition that supports anonymous user access.

**Anonymous External User (IBI\_ANONYMOUS\_EXTERNAL\_USER)**

If set, specifies the user ID used to obtain authorization for the anonymous user from an external security provider.

**Note:** This setting is relevant only to the Enterprise Edition, which is the only edition that supports anonymous user access.

**Named Anonymous User (IBI\_NAMED\_ANONYMOUS\_USERS)**

When this check box is selected (True) and your installation of WebFOCUS uses an external or pre-authentication method, named anonymous users are allowed. If the user is not in the repository and does not pass the IBI\_ALLOW\_LOGIN\_EXTERNAL\_GROUPS setting, the sign-in will complete, and the user will have the same authorization as a public user within WebFOCUS. The user will not be added to the database and cannot be added to any groups or be shared with. Such users are considered public users within WebFOCUS, although their user IDs will be tracked in the session monitor. Authorization on the Reporting Server is based on the explicit user ID. The default value is False (check box cleared).

If the user is registered in WebFOCUS, but no longer passes the IBI\_ALLOW\_LOGIN\_EXTERNAL\_GROUPS setting, the user will still be treated as a named anonymous user.

**Note:** This setting is relevant only to the Enterprise Edition, which is the only edition that supports anonymous user access.

**Enable Password Change (IBI\_USER\_PASSWORD\_CHANGE)**

The default value is True (check box is selected), which enables users to change their own passwords. You may wish to disable this ability under certain circumstances. For example, your system may authenticate users against an external system that will not allow them to change their passwords through WebFOCUS.

**Add Namespace When Creating Users by Group Administrators (IBI\_USER\_NAMESPACE)**

Used for multi-tenant implementations, where group administrators are allowed to create users for the groups they administer. This setting specifies whether or not a namespace is added as a prefix or suffix to user names when created by a group administrator.

- ☐ When set to (NONE), the default setting, user names do not include a namespace.
- ☐ When set to PREFIX, the namespace, followed by a slash (\), precedes the user name.

For example, if a Group Administrator signs in as tenant1\groupadmin, tenant1 is the namespace for this Group Administrator and all of the users for whom this Group Administrator is responsible. When creating users, the namespace of the Group Administrator is automatically prepended to all new user names when created: tenant1\username.

- ☐ When set to SUFFIX, the namespace, preceded by an at sign (@), follows the user name.

For example, if a Group Administrator signs in as groupadmin@tenant1.com, the namespace of the Group Administrator is tenant1.com. The namespace of the Group Administrator is appended to all new user names when created: username@tenant1.com.

The additional level of identification provided by the use of a namespace helps prevent conflicts when the same name is assigned to users in more than one group, and supports SaaS installations that assign users to multiple Tenant Groups.

### Configuring Security Zones

The Security Tab enables you to configure the type of pre-authentication to use for each of the four security zones. Pages under the Security folder enable you to view and update the configuration for each Security Zone.

The four zones are:

- ☐ **Default Zone.** Defines authentication methods for all requests not processed by one of the other zones.
- ☐ **Mobile Zone.** Defines the authentication method for WebFOCUS mobile products, including the WebFOCUS® Mobile App.
- ☐ **Portlet Zone.** Defines the authentication method for WebFOCUS Open Portal Services products, including SharePoint.
- ☐ **Alternate Zone.** Defines an alternate authentication method for requests within the same installation of WebFOCUS.

### Understanding the Default Zone Configuration

The Default Zone establishes the type of authentication for most users.

By default, the Authentication page in the Default Zone is configured to accept Form Based and Anonymous Authentication settings. Form Based security can be based on Internal Portal Security or External Security (WFRS). The Form Based setting presents users with a Sign in page whenever they open WebFOCUS. The public user defined in the Anonymous Authentication profile permits WebFOCUS to accept all users with or without passwords. This default configuration accommodates the broadest range of users. However, Administrators can enable or disable any of the authentication methods on this page to upgrade this configuration to a level of authentication that best supports their requirements.

By default, the Request Matching page in the Default Zone is configured to accept all Request URL Patterns and IP Address Patterns. The Request Matching page should not be changed, but you can modify the IP Addresses to use for this default zone.

### **Understanding the Mobile Zone Configuration**

The Mobile Zone offers authentication methods tailored to the higher level of security required by users who access WebFOCUS from mobile devices. This zone allows Administrators to use one of the established authentication methods within WebFOCUS for Mobile users.

The Authentication page in the Mobile Zone is configured to accept Form Based and Remember-Me settings, by default. These settings present users with a Sign in page whenever they open WebFOCUS and the Remember-Me Authentication profile permits WebFOCUS to allow users to maintain trusted access to WebFOCUS through multiple sessions. Administrators can enable or disable any of the authentication methods on this page.

The Request Matching page in the Mobile Zone limits URL Requests to two patterns, /Mobile Controller/\*\*, and /Mobile Favs Controller/\*\*. Neither URL Request patterns nor IP Addresses can be added, removed, or edited.

### **Understanding the Portlet Zone Configuration**

The Portlet Zone offers authentication methods tailored to the higher level of security required by remote users who access WebFOCUS from WebFOCUS Open Portal Services products, including SharePoint.

The Authentication page in the Portlet Zone is configured to accept Form Based and Remember-Me settings, by default. These settings present users with a Sign in page whenever they open WebFOCUS and the Remember-Me Authentication profile permits WebFOCUS to allow users to maintain trusted access to WebFOCUS through multiple sessions. You can enable or disable any of the authentication methods on this page.

The Request Matching page in the Portlet Zone limits URL Requests to a single pattern, /tool/portlets/\*\*. Neither URL Request patterns nor IP Addresses can be added, removed, or edited.

### **Understanding the Alternate Zone Configuration**

The Alternate Zone allows Administrators to sign in using a different method of authentication from the Default Zone. Administrators can use the Alternate Zone to customize the methods of authentication that can be used to support users.

The Authentication page in the Alternate Zone is configured to accept Form Based Authentication, by default. This setting presents users with a Sign in page whenever they open a session. You can enable or disable any of the authentication methods on this page. To establish an alternate method of authentication, disable the two default methods, and enable a method that is not in use in the default zone.

The Request Matching page in the Alternate Zone permits you to add URL Request Patterns and IP Address Patterns to limit the range of valid URLs to support authentication. By default, the URL Request Patterns page displays the pattern, `/**`, that accepts any and all URL layouts. The IP Address pattern page displays three patterns, `127.0.0.1`, `0:0:0:0:0:0:1`, and `::1`, all representations of the LocalHost IP address in IPV4 and IPV6 respectively.

### Enabling Security Zones

All security zones except the Alternate Zone are enabled, by default. You must enable the Alternate Zone to use it. To enable a Security Zone, change the status of that zone on the Security Zones page from Disabled to Enabled.

#### ***Procedure:*** How to Enable a Security Zone

On the Security Zones Page, click anywhere in a Security Zone entry marked Disabled, and then, in the Actions section, click *Enable*.

The status changes from Disabled to Enabled, and the Security Zone is ready for use.

### Working With the Authentication Page

The Authentication page defines the methods of authentication available within a security zone. The default settings for each zone identify the most commonly used authentication methods for users in that zone, but Administrators can replace or supplement them with any of the other methods on the Authentication page.

Each available authentication method requires a unique configuration and works in different ways to authenticate users. Authentication methods that are available to users within a specific zone are identified with a check mark and a status of Enabled. Methods that are not available are marked with a status of Disabled.

The Actions section of the Authentication page contains links to the dialog boxes and activities that affect all Authentication methods in a particular zone. The Security Zones section contains links that save, export, or import Authentication page settings.

The Options link opens the Authentication Options dialog box where administrators can identify a customized URL to which WebFOCUS can direct users after their logout.

The Key Management link opens the Key Management dialog box where administrators can configure the location of the Keystore file that identifies the secure keys that support certificate-based methods of authentication, such as SAML and Trusted Ticket.

The Cross-Origin Settings link opens the Cross-Origin Settings dialog box, where administrators can configure WebFOCUS to allow the use of its resources in external applications that take advantage of WebFOCUS business intelligence by embedding WebFOCUS content and resources into their webpages. Within this dialog box, the Allow Embedding check box supports the embedding of WebFOCUS resources in the webpages of comma-delimited whitelisted URLs. The Allow Cross-Origin Resources Sharing (CORS) check box supports the use of Ajax request and response messages that enable users of comma-delimited whitelisted URLs to interact with embedded WebFOCUS resources. Each zone maintains its own configuration of cross-origin settings.

The Enable/Disable link enables previously disabled authentication methods, and disables previously enabled methods. This link becomes available only after an authentication method is selected.

The Edit link opens the dialog box that supports a selected Authentication Method. In that dialog box, you can create or update the configuration settings required by that method. This link becomes available only after an authentication method is selected.

**Procedure: How to Enable an Authentication Method**

1. On the Authentication Page, right-click the *Name* or *Status* section of an Authentication Method entry marked Disabled, and then click *Enable*.
- or
2. Click anywhere in an Authentication Method entry marked Disabled, and then, in the Actions section, click *Enable*.

The status changes from Disabled to Enabled with a check mark, and the method of authentication represented by that entry is available for use within the Security Zone.

**Procedure: How to Disable an Authentication Method**

1. On the Authentication Page, right-click the *Name* or *Status* section of an Authentication Method entry marked Enabled, and then click *Disable*.
- or
2. Click anywhere in an Authentication Method entry marked Enabled, and then, in the Actions section, click *Disable*.

The status changes from Enabled to Disabled, the check mark clears, and the method of Authentication represented by that entry is no longer available for use within the Security Zone.

**Procedure: How to Save Changes to the Authentication Page**

1. On the Authentication Page, in the Actions section, under Security Zones, click Save.
2. When you receive a confirmation message, click *OK*.
3. When you receive a message to reload the web application, click *OK*.
4. Sign out of your current session, sign in again as an administrator, and return to the Administration Console.
5. Click the *Security Tab*, and under the Security ZoCross-ne Folder, click the Authentication Page for the zone that you recently configured.

Your new or updated settings appear as configured.

**Procedure: How to Configure a Custom Logout Address**

Security Zones are configured to use form-based authentication, by default. When users in a form-based authentication security zone sign out, the Sign out page that opens links users to the Sign in page. However, in zones that use an external authentication method or a pre-authentication method, there is no need to link users to the Sign in page after they sign out. For these zones, the Custom Logout Address substitutes the URL of an alternative sign-out page that overrides the display of the default Sign out page.

1. On the Authentication page, in the Actions section, click *Options*.
2. In the Authentication Options dialog box, select the *Enable custom logout target URL* check box.
3. Type the custom logout target URL.
  - ☐ If the Security Zone is configured for Integrated Windows Authentication (IWA), accept the default sign-out URL, */signout*.
  - ☐ If the Security Zone is configured for another third party pre-authentication provider, type the sign-out URL that ends the SSO product session for that provider, if one exists. For example, the sign-out URL for WebSEAL may be:

<http://webseal.domain.com/pkmslogout>

The sign-out URL for Siteminder may be:

<http://siteminder.domain.com/logout.html>



To return a user working in a single sign on environment to his or her original portal automatically, leave the final term blank. For example, the sign-out URL for WebSEAL would then be:

<http://webseal.domain.com>

4. Click OK.

## Managing the Allowed Host Names List

In WebFOCUS internal communications, user requests move from browsers to the WebFOCUS Reporting Server in the form of HTTP Request messages. By convention, HTTP Request messages must identify the URL of the virtual host, which is the application or website hosted on the server that will process the request, in their Host Header field. Messages from legitimate users identify the URL of an existing host on their targeted server. However, messages from potential attackers can identify URLs for hosts that do not exist on the targeted server.

Servers that do not require the authentication of the host header URL of incoming HTTP Request messages typically direct those that contain the URL of an undefined host to the first available host application for processing. That host then processes the message containing the unrecognized URL, substitutes it for the legitimate URL in the Location field in the Web Cache, and returns messages containing this poisoned content from the cache. Any following messages are then redirected to the URL introduced by the attacker and allow that server to return a message that contains malicious code to the sender.

To protect against these HTTP response header injection attacks, administrators must create an allowed list of valid host names for each active security zone. The Host Header URLs from incoming request messages can then be validated against this list.

After an allowed list is established, the WebFOCUS Reporting Server accepts only incoming HTTP Request Messages that contain a URL that appears on this list and returns an error message stating that the resource did not process correctly for all other messages.

Administrators can define a list of allowed host names for their organization in the *Allowed host names* field of the *Authentication Options* dialog box. By default, this field contains an asterisk (\*) wild card, which accepts incoming HTTP Request messages directed to all host name URLs. We recommend that you accept this option only if you have incorporated an independent application that validates host names in HTTP Request Headers before they are accepted by the WebFOCUS Reporting Server.

**Procedure: How to Configure the Allowed Host Names List**

To restrict the acceptance of incoming HTTP Request messages within a security zone to those that contain the URL of an existing virtual host on the WebFOCUS Reporting Server, administrators must replace the asterisk (\*) wildcard character in the *Allowed host names* field of the *Authentication options* dialog box with a comma-separated allowed list of the URLs of virtual hosts, web sites, or applications, located on the WebFOCUS Reporting Server. URLs in the host header field of incoming HTTP Request messages must match a URL in this list to be accepted.

1. In the Administration Console, select the *Security* tab.
2. On the *Security* tab, expand the folder for the Security Zone that contains the Allowed Host Names list you wish to configure, and select the *Authentication* page node.
3. In the Actions section of the Authentication page, select *Options* to open the Authentication Options dialog box.
4. Enter the URL for each virtual host that is defined on the WebFOCUS Reporting Server and is allowed to process incoming HTTP Request messages in the *Allowed host header* field.
  - ☐ You can enter a fully qualified URL to represent a single host name. For example, *www.samplehost.com*. Matches against fully qualified URLs must be exact and are case-sensitive.
  - ☐ You can also use a period (.) as a wildcard to represent a range of host names. For example, the wildcard in the *.ibi\_apps.com* URL would match *www.ibi\_apps.com*, *www.server1.ibi\_apps.com*, and any other URL that contains characters preceding *ibi\_apps.com*.
  - ☐ If you must list multiple URLs in this field, separate each URL with a comma.
5. Delete any URLs that are outdated or no longer allowed.
6. Select *OK* to save the list.
7. On the Authentication page, in the Security Zones section, select *Save*.
8. When you receive a message stating that the web security configuration data was saved successfully, select *OK*.
9. When you receive a message advising you to reload the web application in order for these changes to take effect, select *OK*.
10. Sign out of your current session.
11. Stop and restart the WebFOCUS Reporting Server.
12. Sign in again as an administrator and test the new configuration.

## Configuring Cross-Origin Settings

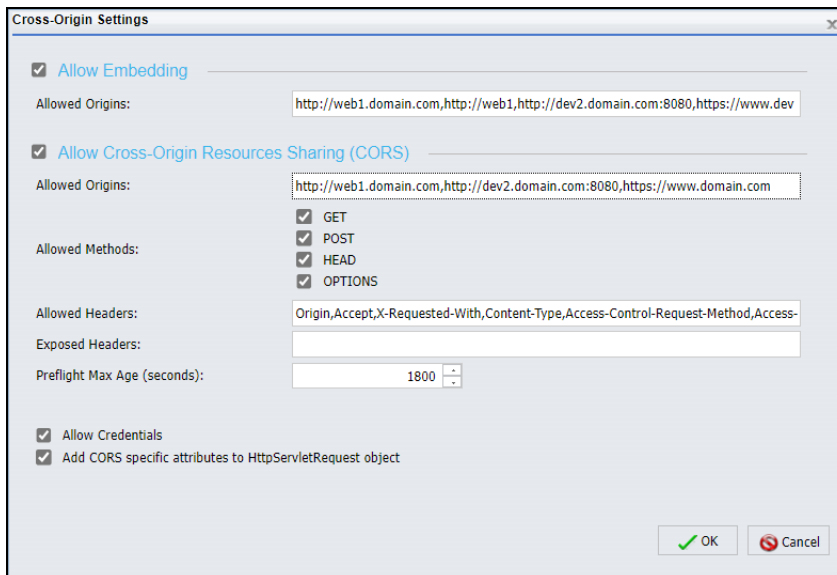
External applications can take advantage of WebFOCUS business intelligence by embedding WebFOCUS content and resources into their webpages. For example, an external application designed to provide customer service can embed portals designed and built within WebFOCUS that add reporting, charting, and analytic resources to the customer service metrics or account service history information they display.

However, to protect WebFOCUS from requests to embed its resources or content from unknown and unauthorized external applications, WebFOCUS does not allow embedding, by default. By selecting the *Allow Embedding* check box in the Cross-Origin Settings dialog box, an administrator can override this default configuration, and allow WebFOCUS to accept requests to embed portals, pages, or other resources into a frame or iframe within the webpage of a trusted external application.

External applications can also take advantage of WebFOCUS business intelligence by making embedded WebFOCUS content and resources interactive. Asynchronous Ajax requests issued from the browsers of users of the embedded application retrieve or update WebFOCUS resources and content dynamically, keeping information current and allowing for user interaction with embedded content.

Cross-origin resource sharing (CORS) allows a web page to request restricted resources from another domain outside of the domain from which the first resource was served. Using a cross-origin resource sharing policy configuration, a web page may be permitted to embed cross-origin images, stylesheets, scripts, iframes, and videos from separate domains, but forbid more sensitive cross-domain requests, such as Ajax requests. Because it allows a resource to limit cross-origin requests to a specific set of domains and messages, the CORS standard defines a way in which a browser and server can interact to determine whether or not it is safe to allow a cross-origin request. It allows for more freedom and functionality than purely same-origin requests, but is more secure than simply allowing all cross-origin requests. It is a recommended standard of the W3C consortium. For more information see, [https://en.wikipedia.org/wiki/cross-origin\\_resource\\_sharing](https://en.wikipedia.org/wiki/cross-origin_resource_sharing) and the Cross-Origin Resource Sharing Recommendation from the W3C consortium <http://www.w3.org/TR/cors/>.

The Cross-Origin Settings dialog box activates the use of Embedding and Cross-Origin Resource sharing within WebFOCUS, as shown in the following image. The Allow Embedding check box supports the basic request to embed content within a frame or iframe of an external webpage. The Allow Cross-Origin Resources Sharing (CORS) check box supports the use of Ajax cross-origin sharing requests.



The image shows a 'Cross-Origin Settings' dialog box with the following fields and options:

- ☒ **Allow Embedding**
  - Allowed Origins:
- ☒ **Allow Cross-Origin Resources Sharing (CORS)**
  - Allowed Origins:
  - Allowed Methods:
    - ☒ GET
    - ☒ POST
    - ☒ HEAD
    - ☒ OPTIONS
  - Allowed Headers:
  - Exposed Headers:
  - Preflight Max Age (seconds):
- ☒ Allow Credentials
- ☒ Add CORS specific attributes to HttpServletRequest object

Buttons: OK, Cancel

**Note:** Even though the Allow Embedding and Allow Cross-Origin Resources Sharing (CORS) check boxes appear together in the Cross-Origin Settings dialog box and work together to support the full requirements of Embedded BI Applications, these two settings are not dependent on each other. For example, an installation of WebFOCUS can be configured to support an external application that uses cross-origin resource sharing but does not require the use of embedded WebFOCUS content in a frame or iframe. Another installation of WebFOCUS could be configured to support an simple application that embeds a portal in a frame or iframe, but does not support cross-origin Ajax requests.

## Defining Origins

In the Cross-Origin Resource Sharing standard, an origin is defined by the scheme, host, and port of a URL. The Scheme identifies the protocol of the host it represents, typically `http://` or `https://`. The Host identifies the registered name (including but not limited to a hostname), or IP address of the host. The Port identifies the endpoint of communications for the host.

As long as these three components are effectively the same, the URL defines the same origin. For example, both of the following resources have the same origin, even though the host component of the second resource URL contains additional path information:

- ☐ `http://example.com/`
- ☐ `http://example.com/path/file/`

However, in the following examples, each of the resources has a different origin from the others:

- ☐ `http://example.com/`
- ☐ `http://example.com/8080/`
- ☐ `http://www.example.com/`
- ☐ `https://example.com:80/`
- ☐ `https://example.com/`
- ☐ `http://example.org/`
- ☐ `http://ietf.org/`

In each case, at least one of the scheme, host, and port components differs from others in the list. For more information, see <https://tools.ietf.org/html/rfc6454>.

## Allowing Embedding

The Allow Embedding check box determines whether or not requests to embed content within a frame or iframe on the webpage of an external application are allowed. When this check box is selected, the Allowed Origins field beneath it defines the range of applications that are allowed to embed WebFOCUS content.

TIBCO WebFOCUS either allows or prevents embedding by assigning specific values to the X-Frame-Options ALLOW-FROM header or to the Content-Security-Policy header of the message it sends in response to a request for embedded content. The specific response header used depends upon the type of browser requesting the resource. The values in the Allow Embedding check box and the Allowed Origins field associated with it are assigned to these response headers.

By default, the Allow Embedding check box is cleared, and WebFOCUS assigns the SAMEORIGIN value to the response header, which will prevent WebFOCUS from embedding resources within a frame or iframe in an external application.

The Allowed Origins field contains the asterisk wild card character (\*), by default. When the Allow Embedding check box is selected, and the Allowed Origins field contains the asterisk wild card character (\*), the ALLOW-FROM or Content-Security-Policy header is excluded from the response message, allowing its content to be embedded in *all* third party applications.

To limit the range of external applications that are allowed to embed TIBCO WebFOCUS resources, an administrator must replace the asterisk (\*) wild card character in the Allowed Origins field with a comma-separated whitelist of URLs that host the specific origins that TIBCO WebFOCUS supports. Every URL in the whitelist must contain the scheme, hostname, and port of the external host. The port should be excluded if the URL uses the default port for the protocol it uses in the scheme, port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

When the Allow Embedding check box is selected, and the Allowed Origins field contains a specific URL or a comma-delimited whitelist of URLs, TIBCO WebFOCUS assigns the whitelist of Allowed Origins, depending on the type of browser that issued the request, to the response header. This setting allows only the specific hosts identified in that whitelist to embed TIBCO WebFOCUS content.

Permission to allow embedding varies by security zone. This feature ensures that embedding can be limited to those security zones that support requests from external applications, and prohibited in those security zones that do not.

The Allow Embedding setting only supports the placement of webpages within a frame or iframe. The separate Allow Cross-Origin Resources Sharing (CORS) request supports the request to retrieve or update resources or content within a webpage. For more information see, [Allowing Cross-Origin Resource Sharing](#) on page 164.

For more information about Embedded BI Applications, see the *TIBCO WebFOCUS Embedded Business Intelligence User's Guide*.

### ***Procedure:*** How to Allow Embedding for a Security Zone

1. In the Administration Console, click the *Security* tab.
2. On the Security tab, under the Security Zones folder, click the *Authentication* node for the zone that will support embedded BI applications.

Most installations assign this configuration to the Default Security zone, but they may also use the Alternate Security zone if they do not use the Default Security zone to support embedded BI applications.

3. On the Authentication page, click *Cross-Origin Settings*.

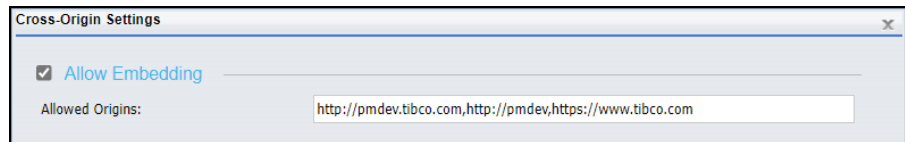
4. In the Cross-Origin Settings dialog box, select the *Allow Embedding* check box, as shown in the following image.



5. To allow HTTP requests and responses from all applications, accept the asterisk (\*) wild card character in the Allowed Origins field under the Allow Embedding check box.
6. To allow HTTP requests and responses from specific applications, type the URL for each allowed application in the Allowed Origins field under the Allow Embedding check box.

When typing URLs in this field, keep the following requirements in mind:

- ☐ You must include the scheme, meaning the term *http:* or *https:*, in each URL.
- ☐ If you use URLs in the format *http://hostname.domain.com* or *http://hostname* to access websites within your network, you must include both URLs in the whitelist.
- ☐ If you include multiple URLs in the whitelist, you must separate each one with a comma, as shown in the following image.



- ☐ Add a port number only to those URLs that do *not* use the default http or https port of 80 or 443, respectively. Port 80 identifies the port for all Hypertext Transfer Protocol HTTP services, and port 443 identifies the port for all HTTP secure services. Therefore, if the scheme of a URL is http and the port is 80, the port does not need to be included. Similarly if the scheme is https and the port is 443, the port does not need to be included.
7. Click OK.

To activate cross-origin resource sharing for external applications, see [How to Allow Cross-Origin Resource Sharing for a Security Zone](#) on page 165.

For more information about the configuration of Embedded BI Applications, see the *WebFOCUS Embedded Business Intelligence User's Guide*.

## Allowing Cross-Origin Resource Sharing

The Allow Cross-Origin Resources Sharing (CORS) check box determines whether or not TIBCO WebFOCUS allows cross-origin sharing requests for content or resources from external applications. When this check box is selected, the Allowed Origins field beneath it defines the range of applications that are allowed to deliver cross-origin sharing requests.

TIBCO WebFOCUS either allows or prevents cross-origin sharing by assigning specific values to the Access-Control-Allow-Origin header of the message it sends in response to Ajax messages requesting cross-origin sharing. The values in the Allow Cross-Origin Resources Sharing (CORS) check box and the Allowed Origins field associated with it define the values that are assigned to this response header.

By default, the Allow Cross-Origin Resources Sharing (CORS) check box is cleared, and TIBCO WebFOCUS responds to cross-origin sharing requests with an HTTP 403 error message, which prevents TIBCO WebFOCUS from sharing resources with an external application.

The Allowed Origins field contains the asterisk wild card character (\*), by default. When the Allow Cross-Origin Resources Sharing (CORS) check box is selected, and the Allowed Origins field contains the asterisk wild card character (\*), TIBCO WebFOCUS assigns the wild card character to the Access-Control-Allow-Origin response header allowing its resources to be available to all external applications.

To limit the range of external applications that are allowed to share TIBCO WebFOCUS resources, an administrator must replace the asterisk (\*) wild card character in the Allowed Origins field with a comma-separated whitelist of URLs that host the specific origins that TIBCO WebFOCUS supports. Every URL in the whitelist must contain the scheme, hostname, and port of the external host. The port should be excluded if the URL uses the default port for the protocol it uses in the scheme, port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

When the Allow Cross-Origin Resources Sharing (CORS) check box is selected, and the Allowed Origins field contains a specific URL or a comma-delimited whitelist of URLs, TIBCO WebFOCUS assigns the whitelist of Allowed Origins to the Access-Control-Allow-Origin response header. This setting allows TIBCO WebFOCUS to share resources only with the specific hosts identified in that whitelist in response to Ajax request messages.



Once activated, the remaining features establish a standard set of protections over the use of cross-origin resources for those embedded applications supported by the security zone, as shown in the following image.

☒ Allow Cross-Origin Resources Sharing (CORS)

Allowed Origins:

Allowed Methods:

- ☒ GET
- ☒ POST
- ☒ HEAD
- ☒ OPTIONS

Allowed Headers:

Exposed Headers:

Preflight Max Age (seconds):

Settings in this dialog box incorporate all of the features that the cross-origin resource sharing specification will support, such as URLs, request methods, headers, and credentials. They also define the maximum time by which preflight requests must be completed.

Permission to allow cross-origin resource sharing varies by security zone. This feature ensures that cross-origin resource sharing can be limited to those security zones that support requests from external applications, and prohibited in those security zones that do not.

The Allow Cross-Origin Resources Sharing (CORS) check box only supports the use of cross-origin requests to retrieve or update resources or content within a webpage. The separate Allow Embedding request supports the request to embed content within a frame or iframe in an external application webpage. For more information see, [Allowing Embedding](#) on page 161.

For more information about Embedded BI Applications, see the *TIBCO WebFOCUS Embedded Business Intelligence User's Guide*.

### **Procedure: How to Allow Cross-Origin Resource Sharing for a Security Zone**

1. In the Administration Console, click the *Security* tab.
2. On the Security tab, under the Security Zones folder, click the *Authentication* node for the zone that supports embedded applications.

Most installations assign this configuration to the Default Security zone, but they may also use the Alternate Security zone if they do not use the Default Security zone to support Embedded BI Applications.

3. On the Authentication page, click *Cross-Origin Settings*.
4. In the Cross-Origin Settings dialog box, select the *Allow Cross-Origin Resources Sharing (CORS)* check box.

Settings in the dialog box become available, as shown in the following image.

5. Type the URL for each application that is allowed to issue cross-origin resource sharing requests to TIBCO WebFOCUS in the Allowed Origins field under the Allow Cross-Origin Resources Sharing (CORS) check box.

When typing URLs in this field, keep the following requirements in mind:

- ☐ You must include the scheme, that is, the term *http:* or *https:*, in each URL.
- ☐ If you use URLs in the format *http://hostname.domain.com* or *http://hostname* to access websites within your network, you must include both URLs in the whitelist.
- ☐ If you include multiple URLs in the whitelist, you must separate each one with a comma, as shown in the following image.

- ☐ Add a port number only to those URLs that do *not* use the default http or https port of 80 or 443, respectively. Port 80 identifies the port for all Hypertext Transfer Protocol HTTP services and port 443 identifies the port for all HTTP secure services. Therefore, if the scheme of a URL is http and the port is 80, the port does not need to be included. Similarly if the scheme is https and the port is 443, the port does not need to be included.
6. Accept the default values assigned to all of the remaining fields and check boxes.

When your configuration is complete, the dialog box will resemble the following image.

The image shows a 'Cross-Origin Settings' dialog box with the following configuration:

- ☒ **Allow Embedding**
  - Allowed Origins: `http://web1.domain.com,http://web1,http://dev2.domain.com:8080,https://www.dom`
- ☒ **Allow Cross-Origin Resources Sharing (CORS)**
  - Allowed Origins: `http://web1.domain.com,http://dev2.domain.com:8080,https://www.domain.com`
  - Allowed Methods:
    - ☒ GET
    - ☒ POST
    - ☒ HEAD
    - ☒ OPTIONS
  - Allowed Headers: `Origin,Accept,X-Requested-With,Content-Type,Access-Control-Request-Method,Access-`
  - Exposed Headers: (empty field)
  - Preflight Max Age (seconds): `1800`
  - ☒ Allow Credentials
  - ☒ Add CORS specific attributes to HttpServletRequest object

Buttons: OK, Cancel

7. Click OK.

For more information about the configuration of Embedded BI Applications, see the *TIBCO WebFOCUS Embedded Business Intelligence User's Guide*.

## Configuring HTTP Strict Transport Security (HSTS) Within a Security Zone

The HTTP Strict Transport Security Settings link connects you to the HTTP Strict Transport Security Settings dialog box, where you can implement the use of an HSTS security policy for your selected Security Zone. This policy calls for the use of TLS (SSL) level security on all communications between browsers assigned to individual users and the Application Server. Therefore, it is relevant only to those organizations that have configured the use of TLS (SSL) security. For more information, see [Configuring TIBCO WebFOCUS for SSL](#) on page 51.

An HTTP Strict Transport Security (HSTS) policy is a security enhancement issued by a server that requires the use of the https protocol for all incoming requests. When this policy is in place, the server that hosts a website responds to the first request from a browser that does not use the https protocol by returning a message with a response header that contains the Strict-Transport-Security field. The presence of this field in the response header indicates that the server will not accept any further requests from that browser that do not arrive over an https connection.

The response header can also include a field identifying the time limit, typically one year, over which the policy will be enforced. Any subsequent requests from that browser that do not use this protocol will receive an error message in response.

When the browser receives a message with a response header that contains a Strict-Transport-Security field, it knows to use the https protocol when sending any future messages to the site. The browser also knows that any other site using the same name that does not require the use of this protocol is not legitimate, and it automatically redirects requests to the site that does require the use of the https protocol.

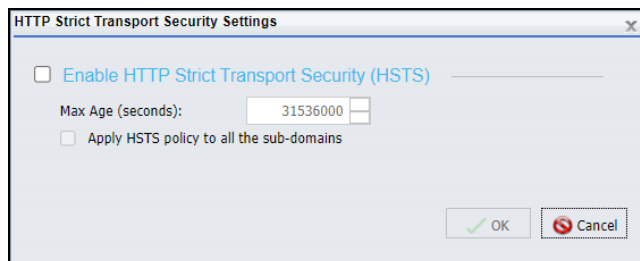
By imposing this policy within a Security Zone, you introduce this extra level of security to all communications between users in that zone and the Application Server. The policy ensures that all communications within that zone use the https protocol and are therefore encrypted and validated by a public key certificate. It also helps prevent requests from users in that zone from being inadvertently misdirected to an illegitimate site that does not require the https protocol.

A link to the HTTP Strict Transport Security Settings dialog box and its configuration appears on the Authentication page of the Administration Console Security tab. Because the policy only applies to the zone in which it is configured, you will need to establish this policy for each of the security zones in which it will apply. As a best practice, we recommend the use of the HSTS policy for all security zones in installations that have been configured to use TLS (SSL) security.

### *Understanding the HTTP Strict Transport Security Setting Dialog Box*

The HTTP Strict Transport Security Settings dialog box enables the HSTS policy for a selected Security Zone. Additional settings define the length of time that the policy is enforced and whether or not the policy extends to messages directed to subdomains within the host server URL.

HTTP Strict Transport Security is not enabled, by default, for any security zone, therefore the features in this dialog box remain unavailable until you select the Enable HTTP Strict Transport Security (HSTS) check box.



When selected, the Enable HTTP Strict Transport Security (HSTS) check box activates the HSTS policy for the security zone selected in the left pane of the Security tab. When this check box is selected, the other features in the dialog box become available.

The Max Age (seconds) list contains the number of seconds for an entire year, by default. You can increase or decrease this value to conform to the standards of your organization.

The Apply HSTS policy to all the sub-domains check box is cleared, by default. However, we recommend that you select it in order to ensure that messages directed to all subdomains in the site hosting the Application Server are required to use the https protocol.

### **Procedure: How to Configure HSTS Security for a Security Zone**

This configuration is relevant only if you have also configured the use of TLS (SSL) in internal communications. For more information, see [Configuring TIBCO WebFOCUS for SSL](#) on page 51.

1. Sign in as an administrator, open the Administration Console, and select the Security tab.
2. On the Security tab, under the Security Zones folder, select the Authentication node for the zone in which you will enable HSTS.

If you have configured TIBCO WebFOCUS to use https, we recommend that you enable this feature for all security zones in use within your installation.

3. On the Authentication page, select *HTTP Strict Transport Security Settings* to open the HTTP Strict Transport Security Settings dialog box.
4. Select the *Enable HTTP Strict Transport Security (HSTS)* check box.
5. Accept the default value of 31536000 in the Max Age (seconds) field to establish the use of HTTP Strict-Transport-Security for a full year.

You can use the up or down arrows to the right of this field to increase or decrease the number of seconds in this value.

6. Select the *Apply HSTS policy to all the sub-domains* check box to add the requirement that all requests to subdomains within the Application Server use the https protocol.
7. Select OK to save your configuration.
8. Save changes to the Security Zone as described in [How to Save Changes to the Authentication Page](#) on page 156.

## Understanding the Request Matching Page

The Request Matching page defines the range of authentic URLs and IP addresses for a Security Zone. The page contains two tabs, Request URL Pattern, and IP Address of Client/Last Proxy. These tabs identify the patterns of URLs and IP Addresses of trusted users. A pattern can be very general to include a wide range of URLs and IP Addresses, or it can be very precise to limit valid requests to a few URLs and IP Addresses. When configured for a Security Zone, settings on the Request Matching page tabs exclude all request messages except those that match the pattern of trusted URLs and IP Addresses. By excluding requests from untrusted locations, the Request Matching pages help prevent potentially malicious requests from compromising WebFOCUS operations.

Request URL patterns use the following Java Ant path patterns.

- ☐ All elements in the URL pattern are separated with forward slashes.
- ☐ A single question mark (?) represents a single character.
- ☐ A single asterisk (\*) represents a string of zero or more characters.
- ☐ Two asterisks (\*\*) represents zero or more directories in a path.

Do not make modifications to the settings on this page unless instructed to do so by a member of the Customer Support Team.

## Understanding the URL Request Pattern Tab

The Request URL Pattern tab defines the range of URLs that can be accepted as authentic origins for user requests.

The default settings for this tab vary by Security Zone to reflect differences in the security restrictions required by each one. For example, the Mobile and Portlet Security Zones support users who work at remote sites or through a portlet. Their configurations therefore strictly limit the range of acceptable URLs to a few patterns, by default. In contrast, the Default and Alternate Security Zones support all users who work at sites within an organization and their default configurations impose few to no restrictions.

## Understanding the IP Address of the Client/Last Proxy Tab

The IP address of the Client/Last Proxy tab defines the range of client and proxy site IP Addresses that can be accepted as authentic origins for user requests. A proxy site, or proxy server, is a server that acts as an intermediary in all messages exchanged between a user and an application server.

The default settings for this tab vary by zone to reflect differing security restrictions required by each zone. The Default, Mobile, and Portlet zones contain no values for this tab, and the Add, Edit, and Remove links are unavailable, effectively making the evaluation of the client or last proxy IP addresses irrelevant.

By contrast, the IP Address of the Alternate Security Zone contains three default patterns, 127.0.0.1, 0:0:0:0:0:0:1, and ::1. All of these patterns are representations of the LocalHost IP address in IPV4 and IPV6 respectively, limiting the Alternate Security Zone to requests issued from local users. The Add, Edit, Edit Setting and Remove links are also available in this zone. Any configuration of these features will affect only those users who are assigned to the Alternate Zone.

## Importing and Exporting Security Zone Settings

The settings for each security zone are stored in four security configuration files, securitysettings.xml, securitysettings-mobile.xml, securitysettings-portlet, and securitysettings-zone.xml. Before you change the authentication method for a zone, use the Export link on any zone page to save a backup zip file of the security zone configuration. If you need to restore a previous configuration of security zone settings, use the Import link to capture settings from that configuration and restore them to the security configuration files on the server.

### **Procedure:** How to Export Security Configuration Files

The Export link creates a zip copy of the four security configuration files from the server and saves them in a designated network location. Use this operation to backup existing security configuration settings before updating them.

1. On the Authentication or Request Matching page of a Security Zone, in the Actions section, click *Export*.
2. When you receive a message asking you to open the zip file, click *Open*.
3. From the WinZip dialog box menu bar, click *File*, and then click *Save As*.
4. Accept the default name for the file, or type a new name for it.
5. Navigate to the location for the new file, and then click *Save*.
6. From the WinZip dialog box menu bar, click *File*, and then click *Exit*.

### **Procedure:** How to Import Security Configuration File Settings

The Import feature enables you to copy and paste the text of previous versions of the security configuration files into the four security files on the WebFOCUS server. Use this operation whenever you need to restore previously established security configuration settings.

1. On the Authentication or Request Matching page of a Security Zone, in the Actions section, click *Import*.

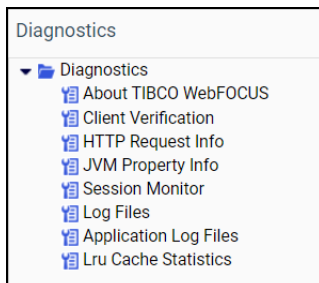
2. In the Import the Web Security Configuration Data dialog box, click the tab that represents the configuration file for the zone that must contain this new configuration data, `securitysettings.xml`, `securitysettings-mobile.xml`, `securitysettings-portlet.xml`, or `securitysettings-zone.xml`.
3. Copy the configuration text from your independent source file.
4. In the Please copy the web security configuration data from your local hard files and paste here box, paste the text from that source file.
5. Click *Apply*.
6. When the confirmation dialog box opens, click *OK* to complete the import.
7. If you receive a message stating that the import failed to parse the input web security configuration data, click *OK*, adjust the text as necessary, and repeat steps 5 and 6.

## Working With TIBCO WebFOCUS Diagnostics

Using the Diagnostics menu of the Administration Console, users whose privileges allow them to view the Administration Console can:

- ☐ View and report on version information.
- ☐ Verify the installation and configuration of client components.
- ☐ Monitor TIBCO WebFOCUS Sessions.
- ☐ Turn logging on or off and view log files.
- ☐ View log files created by separate applications.
- ☐ Monitor LRU cache statistics.

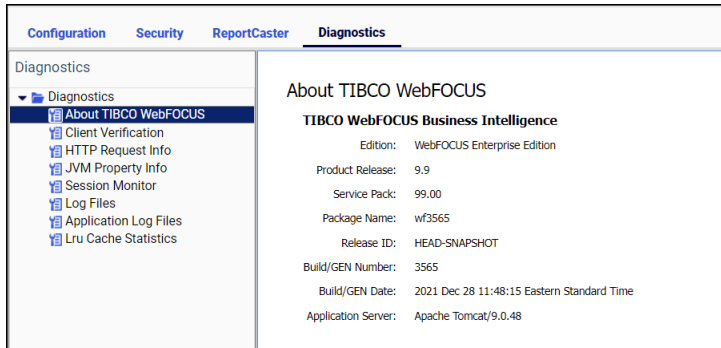
The Diagnostics menu is shown in the following image.





## Reviewing Version Information

The About TIBCO WebFOCUS page displays information about the release you are using and the optional components installed with it, as shown in the following image.



You can use the information on this page to identify your current product release and service pack when corresponding with the Information Builders Customer Support team.

When you select *About TIBCO WebFOCUS*, the following information appears in the main window:

**Edition.** Product edition, for example, WebFOCUS Enterprise Edition.

**Product Release.** Release number, for example, 8.2.

**Service Pack.** Service pack number, for example, 05.01 The first and second digits represent the version number. The third and fourth digits represent the interim release version number.

**Package Name.** Installation file package name, for example, wf032019a.

**Release ID.** Product release number, for example, 8205.

**Build/GEN Number.** Specific product build number, for example, 74.

**Build/GEN Date.** Date and time the build number was generated, for example, March 20, 2019 8:04:35 PM EDT.

**Application Server.** Application Server, for example, Apache Tomcat/8.5.32.

This version of the About TIBCO WebFOCUS page, that opens from the Diagnostics tab, is only available to those users whose privileges allow them to open and review the Administration Console.

However, the product and application server information on this page is also available to those users whose privileges allow them to view the About TIBCO WebFOCUS Business Intelligence window. To open this other window, select *Help*, and then click *About WebFOCUS*.

## Reviewing Client Verification

The Client Verification page displays the current status of client configuration and application settings. When you open this page, the tests required to verify that configuration and application settings are open and available are conducted automatically.

Settings marked pass are available for use. Settings marked fail are not available for use.

The automated verification process includes a validation of web server aliases and directory permissions for each type of client communication mode (CGI, WFServlet, or ISAPI).

The Client verification tools, by default, place the verification logs in the *drive:\ibi\WebFOCUS82\logs* directory. These tools test read, write, and remove permissions for the logs directory. They also test read and write permissions for the *drive:\ibi\WebFOCUS82\config* directory.

To test a Reporting Server connection and the current status of the Graph or Table functionality it can deliver, you must open the Configuration tab, and right-click the icon for the Reporting Server you wish to test. All three tests are available on the shortcut menu assigned to each server node.

### ***Procedure:*** How to Run a Client Verification Test

In the Administration Console, click *Diagnostics*, and then click *Client Verification*.

The Client Verification page displays your directory permissions, such as creating and deleting applications, signing in as the administrator, reading and writing from the standard directories, creating and deleting workspaces, and creating and deleting reports.

**Note:** If you run this test immediately after performing the installation procedure, there might be a delay resulting from a slow or delayed first time initialization of the Tomcat Web Application that supports client operations.

## Monitoring the HTTP Request Info Page

Settings on the HTTP Request Info page display information about the HTTP or HTTPS headers returned to your browser, as shown in the following image.

Application Server:	Apache Tomcat/9.0.48
Remote User:	admin
J2EE Role:	Unknown
HTTP Headers:	
<u>Header Name</u>	<u>Header Value</u>
host	na1.dev.focibx01.dev.tibco.com:25030
connection	keep-alive
upgrade-insecure-requests	1
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image
accept	
accept-encoding	gzip, deflate
accept-language	en-US,en;q=0.9
cookie	WF-JSESSIONID=8B6D18BF22EA9A14804CD5FD3EF608A; maxInactiveI
Cookies:	
<u>Cookie Name</u>	<u>Cookie Value</u>
WF-JSESSIONID	8B6D18BF22EA9A14804CD5FD3EF608A
maxInactiveInterval	7200000
wcSessionID&ibi_apps\$webconsole\$iwaynode_EDASERVE	4F83A41BA5AA0133274D9D15EEA5916601931FA446E6B90C399495FEBD
wcSessionID&ibi_apps\$webconsole\$IWAYNODE_EDASERVE	4F83A41BA5AA0133274D9D15EEA5916601931FA446E6B90C399495FEBD
serverTime	1640801927277
_gcl_au	1.1.1328329980.1638365276

This information is useful for troubleshooting and HTTP header configuration, especially if you integrate Web Server or Application Server security with TIBCO WebFOCUS, or if your Web Server or Application Server uses virtual hosts (HTTP headers). The following information appears on this page.

**Application Server.** Identifies the name and version of the Application Server. For example, Apache Tomcat/9.0.26. Apache Tomcat is included in the product installation, by default, but a different name appears in this entry if your installation uses a different Application Server platform.

**Remote User.** Identifies the name of the user currently signed in to the session.

**J2EE Role.** Contains the value *Unknown*, by default. Typically, the J2EE role is not relevant.

The **HTTP Headers** section lists the fields and default values returned in the response from the Application Server to Browsers assigned to users in response to their initial requests. They define the acceptable operating parameters of the HTTP session.

- ☐ **host.** Identifies the domain name and port of the Application Server. For example, hostsrvr01.companyname.com:25150.
- ☐ **connection.** Identifies the status of the connection. By default, this value is set to Keep-Alive in order to keep the session open even when idle.
- ☐ **upgrade-insecure-requests**

- ❑ **user-agent.** Identifies acceptable browsers. For example, Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko.
- ❑ **accept.** Identifies acceptable media types. For example, text/html, application/xhtml+xml, image/jxr, \*/\*
- ❑ **accept-encoding.** Identifies the acceptable encoding formats that can be used to compress information in the transaction. For example, gzip, deflate.
- ❑ **accept-language.** Identifies acceptable human language codes. For example, en-US.
- ❑ **cookie.** Identifies a set of values returned to the requestor that contain information about the current state of the session. For a detailed description of the typical parameters included in cookies returned to users from the Application Server, see the Cookies section.

The **Cookies** section lists the following information contained in cookies returned from the Application Server during the current session:

- ❑ **WF-JSESSIONID.** Identifies the unique ID of the current session initiated by the request from the user.
- ❑ **maxInactiveInterval.** Identifies the maximum number of seconds during which communications between the server and browser can remain idle. By default, this value is set to 7200000.
- ❑ **wcSessionID&ibi\_apps\$webconsole\$iwaynode\_EDASERVE.**
- ❑ **serverTime.** Identifies the time at which the current session will expire if it remains idle. This value is expressed in Epoch time, which is also known as Unix Time. It is typically equal to the time of the last response message plus the number of seconds assigned to the maximum inactive interval.
- ❑ **\_ga.** Identifies the Google Analytics Client ID assigned to the Application Server.
- ❑ **\_fbp**
- ❑ **\_gcl\_au**
- ❑ **apt.uid.** Identifies the Linux user ID assigned to the Application Server.

## Monitoring the JVM Property Information Page

Settings on the JVM Property Info page display information about the Java Virtual Machine<sup>®</sup>, also called the JVM, which supports your product installation. The JVM exists within the Random Access memory RAM of the machine that hosts the Application Server and Client, and the statistics that appear on this page refer to the performance of this installation.

Information on this page supports the analysis and troubleshooting of the Java environment for TIBCO WebFOCUS web applications and for the resolution of memory or resource issues.

This page contains links to two tabs. The Memory Information (K) tab displays current JVM memory usage statistics and system properties. The Monitoring JVM Performance tab contains a set of graphs that display patterns of memory usage over the previous hour.

This information can also be found in the JConsole monitoring tool, which is accessible in the Java Virtual Machine environment. However, by placing this information within the Administration Console, the JVM Property page saves you the time and effort required to open and access this information directly from Apache Tomcat® or your host server.

## Monitoring the Memory Information (K) Tab

The Memory Information (K) tab displays current memory usage statistics and additional System Properties for the Java Virtual Machine that runs your installation of TIBCO Web FOCUS, as shown in the following image.

[Memory Information \(K\)](#)
[Monitoring JVM Performance](#)

Type	Pool Name	Current Used	Peak Used	Initial	Committed	Maximum	Threshold Count
Heap	*	1,063,500	~	2,097,152	3,368,448	3,728,384	~
	PS Eden Space	161,664	1,223,680	524,800	573,440	1,265,664	n/a
	PS Survivor Space	41,725	300,542	87,040	64,512	64,512	n/a
	PS Old Gen	860,109	988,711	1,398,272	2,730,496	2,796,544	0
Non-Heap	*	284,679	~	2,496	293,952	0	~
	Code Cache	111,194	111,194	2,496	112,064	245,760	0
	Metaspace	157,441	158,139	0	164,480	0	0
	Compressed Class Space	16,042	16,216	0	17,408	1,048,576	0

Note: To set Initial Heap and Maximum Heap size, use the following JVM startup parameters:

- Xms256m will set the Initial Heap size to 256Mb
- Xmx256m will set the maximum Heap size to 256Mb
- XX:MaxPermSize=128m will set the maximum Perm Gen Size to 128Mb

Note: For Development environments, you can set Xms to a value less than Xmx, so memory is acquired dynamically. In a production environment, it is recommended that Xms be equivalent to Xmx, and that this value is 1/4 of available memory. If deploying multiple versions of WebFOCUS within the same JVM, MaxPermSize should be 128m, per deployed WebFOCUS application.

**System Properties:**

awt.toolkit	sun.awt.X11.XToolkit
catalina.base	/bigcfg/839/tomcat
catalina.home	/bigcfg/839/tomcat
catalina.useNaming	true
common.loader	"\${catalina.base}/lib"; "\${catalina.base}/lib/*.jar"; "\${catalina.home}/lib"; "\${catalina.home}/lib/*.jar"
file.encoding	ISO-8859-1
file.encoding.pkg	sun.io
file.separator	/
ignore.endorsed.dirs	
java.awt.graphicsenv	sun.awt.X11GraphicsEnvironment
java.awt.headless	true
java.awt.printerjob	sun.print.PSPrinterJob
java.class.path	/bigcfg/839/derby/lib/derbyclient.jar:/bigcfg/839/tomcat/bin/bootstrap.jar:/bigcfg/839/tomcat/bin/tomcat-juli.jar
java.class.version	52.0
java.endorsed.dirs	/qas/java/jmx64/AdoptOpenJDK/jdk8u212-b03/jre/lib/endorsed
java.ext.dirs	/qas/java/jmx64/AdoptOpenJDK/jdk8u212-b03/jre/lib/ext:/usr/java/packages/lib/ext
java.home	/qas/java/jmx64/AdoptOpenJDK/jdk8u212-b03/jre

## Memory Usage Statistics Table

The table at the top of this tab shows current memory usage statistics for the installation of the Java Virtual Machine on the host that runs the Application Server and Client, as shown in the following image.

Type	Pool Name	Current Used	Peak Used	Initial	Committed	Maximum	Threshold Count
Heap	*	1,063,500	~	2,097,152	3,368,448	3,728,384	~
	PS Eden Space	161,664	1,223,680	524,800	573,440	1,265,664	n/a
	PS Survivor Space	41,725	300,542	87,040	64,512	64,512	n/a
	PS Old Gen	860,109	988,711	1,398,272	2,730,496	2,796,544	0
Non-Heap	*	284,679	~	2,496	293,952	0	~
	Code Cache	111,194	111,194	2,496	112,064	245,760	0
	Metaspace	157,441	158,139	0	164,480	0	0
	Compressed Class Space	16,042	16,216	0	17,408	1,048,576	0

Values in this table show you the amount of memory currently in use in each of the following JVM memory areas.

The **Heap** memory area includes all class instances and arrays loaded into the JVM during run time. Therefore, the amount of memory allocated to the heap varies with the amount of user activity.

In the JVM, an internal Garbage Collection process automatically clears any class instances or arrays that are no longer in use. Classes and arrays that survive this process move from the Eden space, where all new classes and arrays are first loaded, to the Survivor space, and then to the Old Gen space. As a result, the table displays one row of summary statistics for the entire heap and three additional rows of statistics for the following three pools, or memory areas, within the heap.

- ☐ **PS Eden Space.** Contains all new class instances and arrays.
- ☐ **PS Survivor Space.** Contains class instances and arrays that survived the garbage collection process in the Eden Space because they continue to be in use.
- ☐ **PS Old Gen.** Contains class instances and arrays that survived the garbage collection process in the Survivor Space because they continue to be in use.

The **Non-heap** memory area includes all threads and memory required to maintain internal JVM processing. Typically, this area is not subject to garbage collection, and the size of this area does not vary.

The table displays one row of statistics for the entire non-heap memory area and three additional rows of statistics for the following three pools:

- ☐ **Code Cache.** Contains memory used to compile and store native code.
- ☐ **Metaspace.** Contains metadata automatically loaded from classes created by users.

- ❑ **Compressed Class Space.** Contains metadata about Java classes loaded by the applications.

The columns in this table represent the following statistics for each memory area.

- ❑ **Pool Name.** Identifies the name of the memory area to which the statistics in the row apply.
- ❑ **Current Used.** Identifies the amount of memory currently in use, in kilobytes, including the memory occupied by all objects, both reachable and unreachable.
- ❑ **Peak Used.** Identifies the highest amount of memory, in kilobytes, used by the pool at any one time in the session.
- ❑ **Initial.** Identifies the amount of memory, in kilobytes, used by the pool at the start of the session.
- ❑ **Committed.** Identifies the amount of memory, in kilobytes, guaranteed to be available to the pool.
- ❑ **Maximum.** Identifies the maximum amount of memory, in kilobytes, that can be made available to the pool.
- ❑ **Threshold Count.** Identifies the memory usage threshold, in kilobytes.

Note that, instead of a count, the tilde character appears in the Peak Used column and the Threshold Count column for the Heap and Non-Heap rows, as shown in the following image.

Type	Pool Name	Current Used	Peak Used	Initial	Committed	Maximum	Threshold Count
Heap	*	1,063,500	~	2,097,152	3,368,448	3,728,384	~
	PS Eden Space	161,664	1,223,680	524,800	573,440	1,265,664	n/a
	PS Survivor Space	41,725	300,542	87,040	64,512	64,512	n/a
	PS Old Gen	860,109	988,711	1,398,272	2,730,496	2,796,544	0
Non-Heap	*	284,679	~	2,496	293,952	0	~
	Code Cache	111,194	111,194	2,496	112,064	245,760	0
	Metaspace	157,441	158,139	0	164,480	0	0
	Compressed Class Space	16,042	16,216	0	17,408	1,048,576	0

This character indicates that summary statistics in these categories are not relevant to the overall Heap and Non-Heap memory areas. In all other columns, the number of kilobytes that appear in the Heap and Non-Heap rows are equal to the sum of the kilobytes that appear in the three rows beneath.

## Understanding Entry Highlights

Individual entries in the Current Used and Peak Used columns are highlighted when the value in their category exceeds 90% of the maximum amount of memory that can be allocated to the pool, as shown in the Maximum column.

For example, if the number of kilobytes currently in use in the PS Old Gen pool of the heap exceeds 90% the Maximum amount, that entry will be highlighted with a background color, warning you that the number of existing classes in operation is close to the maximum amount of memory allocated to that pool.

Memory Allocation Guidelines

A standardized list of guidelines appears under the memory usage statistics table as shown below. This list advises you of the startup parameters to add to your JVM installation in order to set the optimum memory size for the Java startup parameters. Details in this list do not vary for each installation.

In this section, Xms refers to the -Xms parameter that defines the initial allocation of memory to the heap. Xmx refers to the -Xmx parameter that defines the maximum allocation of memory to the heap. XX refers to XX parameter that defines the minimum heap free ratio and the maximum heap free ratio.

System Properties List

The **System Properties** list appears at the bottom of the page. This list contains relevant parameters defined within the Java Virtual Machine and identifies the values assigned to them in your local installation of the Application Server and Client.

<b>System Properties:</b>	
awt.toolkit	sun.awt.X11.XToolkit
catalina.base	/bigcfg/839/tomcat
catalina.home	/bigcfg/839/tomcat
catalina.useNaming	true
common.loader	"\${catalina.base}/lib","\${catalina.base}/lib/*.jar","\${catalina.home}/lib","\${catalina.home}/lib/*.jar"
file.encoding	ISO-8859-1
file.encoding.pkg	sun.io
file.separator	/
ignore.endorsed.dirs	
java.awt.graphicsenv	sun.awt.X11GraphicsEnvironment
java.awt.headless	true
java.awt.printerjob	sun.print.PSPrinterJob
java.class.path	/bigcfg/839/derby/lib/derbyclient.jar:/bigcfg/839/tomcat/bin/bootstrap.jar:/bigcfg/839/tomcat/bin/tomcat-juli.jar
java.class.version	52.0

For more information about the specific properties listed here, see the Java Toolkit and Java® Virtual Machine Specification for your version of Java at <https://docs.oracle.com/javase/specs/index.html>.

The final four entries in this list are defined within TIBCO WebFOCUS and identify the encoding scheme used by your installation.

- ☐ **System.in Encoding.** Identifies the current code page and encoding used by the Application Server.



- ☐ **System.out Encoding.** Identifies the current code page and encoding used by the Application Server.
- ☐ **Method setCharacterEncoding.** Identifies whether the use of character encoding is implemented or is not implemented.
- ☐ **Available Processors.** The bit-size of the processors assigned to the machine that supports the JVM.

## Monitoring JVM Performance

The Monitoring JVM Performance tab lists four graphs that display changes in usage of the CPU, Memory, Heap Memory, and Non-Heap Memory resources over the previous hour.

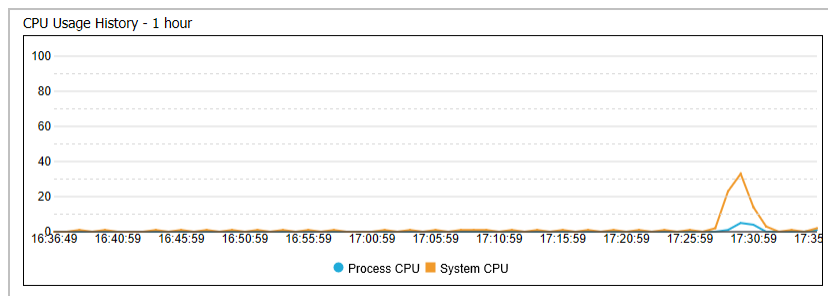
The Refresh button at the top of the page resets the graphs to display behavior from the hour prior to the time you select the button. You can use it to update the graphs to capture the most recent screen behavior.

The Refresh Interval check box and Refresh Interval second(s) field enable you to reset the frequency of the automatic refresh. The Refresh Interval is set to ten seconds, by default. You can replace this value with any number from 1 to 99,999,999. You can activate the automatic refresh by selecting the Refresh Interval check box.

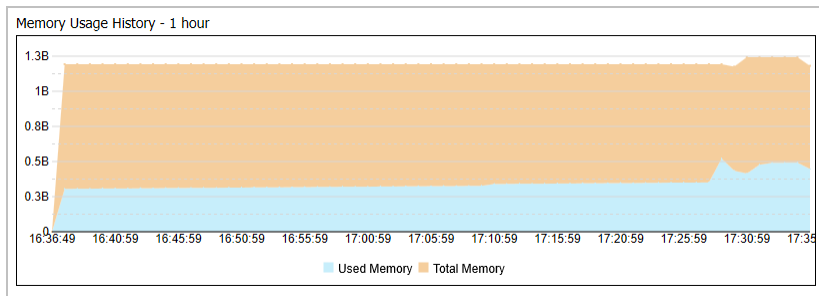
The graphs on this tab support your performance monitoring and troubleshooting by quickly identifying unexpected peaks or troughs in resource usage and when, in the previous hour, they occurred.

**CPU Usage History – 1 hour.** Displays changes in the percentage of CPU resource usage during the previous hour, as shown in the following image.

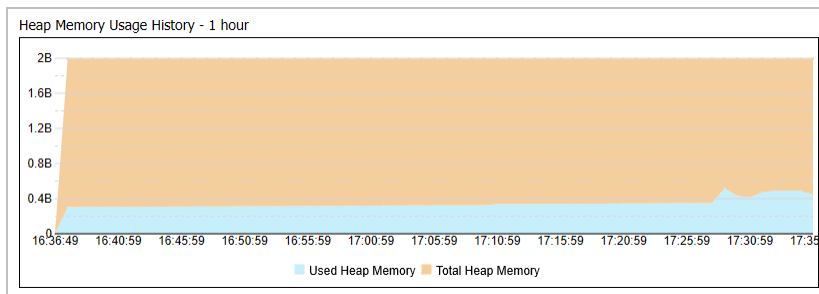
- ☐ **Process CPU.** Displays changes in the percentage of CPU resources used by JVM processes over the specified time period.
- ☐ **System CPU.** Displays changes in the percentage of CPU resources used by operating system processes over the specified time period.



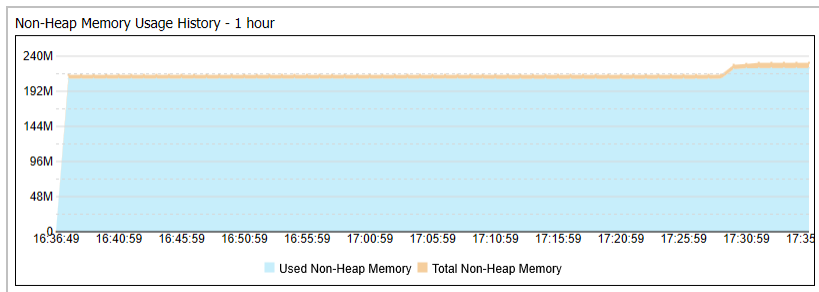
**Memory Usage History – 1 hour.** Displays changes in the number of kilobytes used by the entire JVM application over the previous hour, as shown in the following image. The top entry in the graph displays the total number of kilobytes allocated to memory.



**Heap Memory Usage History – 1 hour.** Displays changes in the number of kilobytes used by the heap memory over the previous hour, as shown in the following image. The top entry in the graph displays the total number of kilobytes allocated to heap memory.



**Non-Heap Memory Usage History – 1 hour.** Displays changes in the number of kilobytes used by the non-heap memory over the previous hour, as shown in the following image. The top entry in the graph displays the total number of kilobytes allocated to non-heap memory.



## Monitoring Sessions

The Session Monitor enables administrators to track all client sessions, as well as connections and activity on the Reporting Server. The Session Monitor displays information about connected users, report requests, and Reporting Server nodes, as shown in the following image.

**Session Monitor**
☐ Refresh interval:  second(s)

URL Logging Level is currently set to 
 Long Running Threshold:  minute(s)

Current Sessions: 5

IP address	Mode	Client User	URL Logging	Trace Control	Trace FEX	Active URLs	URL # / AVG / Max	Server # / AVG / Max	W/ DBMS # / AVG / Max
172.30.234.78	WEB	admin	OFF	Off		1	714 / 0.047 / 3.400	7 / 0.780 / 3.211	4 / 0.001 / 0.001
Last req:EDASERVE/ (17.14.04) -> Run:Fex=ADHOCRCQ									
tlswin10-02.ibi.com	WFDT	admin	OFF	Off		-	185 / 0.072 / 0.478	152 / 0.052 / 0.268	56 / 0.001 / 0.001
Last req:EDASERVE/ (18.15.54) -> Run:Fex=METAQUERY-APPDELETFEILE									
tlswin7e10.ibi.com	WFDT	admin	OFF	Off		-	66 / 0.006 / 0.087	1 / 0.055 / 0.055	0 / 0.000 / 0.000
Last req:EDASERVE/ (15.42.41) -> Run:Fex=METAQUERY-APPSHOWPATH									
qaw7nf03.ibi.com	WFDT	admin	OFF	Off		-	112 / 0.008 / 0.515	1 / 0.063 / 0.063	0 / 0.000 / 0.000
Last req:EDASERVE/ (11.52.34) -> Run:Fex=METAQUERY-APPSHOWPATH									
172.30.236.105	WEB	admin	OFF	Off		-	101 / 0.013 / 0.347	1 / 0.031 / 0.031	0 / 0.000 / 0.000
Last req:EDASERVE/ (10.25.52) -> Run:Domain=Public/App=:SubAct=MR_OLAP:Fex=ADHOCRCQ									

To refresh the information displayed, click the *Refresh* icon. To set an automatic refresh operation, select the *Refresh Interval* check box and accept the default setting of ten second intervals, or type the number of seconds you wish to use instead. If you change the value in this field, it will remain valid only while the Session Monitor page is open. If you close this page and return to it later, the default value will be reestablished.

Administrators can enable or disable logging for all current sessions by clicking *All/None/Selective* next to *URL Logging Level is currently set to*. To enable or disable logging for individual sessions, click *Selective*, and then *On* or *Off* under the URL Logging column for the individual sessions. By default, all log information is located in the `drive:\ibi\WebFOCUS82\logs` directory in Windows or the `install_directory/ibi/WebFOCUS82/logs` in UNIX or Linux.

To prevent inactive sessions from continuing indefinitely, accept the value of five minutes in the Long Running Threshold field, or type a different value to extend or curtail this period. If you change the value in this field, it will remain valid only while the Session Monitor page is open. If you close this page and return to it later, the default value will be reestablished. For each session, the following information is available:

### IP Address

The numerical label assigned to the computer or other device that initiated the session.

Using this address, you can identify the user assigned to the computer or other device that initiated the session.

**Mode**

Identifies the product component that started the session and provides information about all active requests. The product component values are as follows:

**WEB**

Specifies the Client.

**WSRV**

Specifies the Reporting Server.

**WFC**

Specifies the Administration Console.

**WFRQ**

Specifies a report request from a self-service application.

**WFDT**

Specifies App Studio.

**IBFS**

Specifies Information Builders File System.

**Client User**

Specifies the user ID that started the client session. A value of null indicates that it is a request from a self-service application.

**URL Logging**

Enables or disables logging for an individual session or a current user.

**Trace Control**

Enables tracing at a specified level of detail, or disables tracing for a specific IP Address, that is, user.

**Trace FEX**

Identifies whether traces for WFServlet, Client Connector, and Reporting Server are enabled for a session. If tracing is enabled, a *View Trace* icon appears. Click this icon to see the trace.

**Active URLs**

Specifies the number of URLs that are actively in use during the session. This value is relevant only to sessions that are currently open and active. Each URL represents the workstation from which a request was launched to the application server through the browser.

URL

Specifies the number, average duration, and maximum duration of dynamic URLs sent in HTTP requests. Duration is measured in seconds, calculated to the millisecond. Not all URLs in HTTP requests are forwarded to the server, and not all requests forwarded to the server are then forwarded to the DBMS.

Server


Specifies the number, average duration, and maximum duration of dynamic URLs that run reports on the Reporting Server. Duration is measured in seconds, calculated to the millisecond. Not all URLs in HTTP requests are forwarded to the server, and not all requests forwarded to the server are then forwarded to the DBMS.

W/DBMS

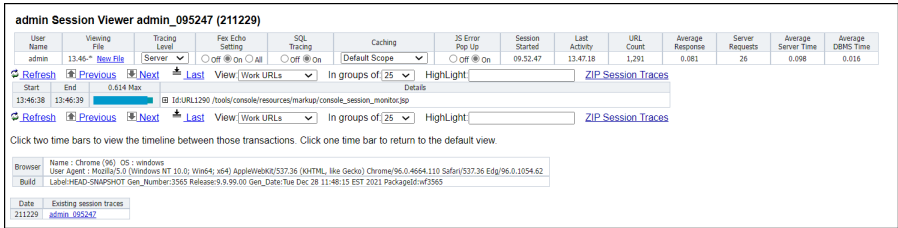
Specifies the number, average duration, and maximum duration of dynamic URLs that run reports against an external database. Duration is measured in seconds, calculated to the millisecond. Not all URLs in HTTP requests are forwarded to the server, and not all requests forwarded to the server are then forwarded to the DBMS.

Procedure: How to Export the Session Monitor Log

You may need to export a session monitor log for troubleshooting.

- 1. In the Administration Console, click the *Diagnostics* tab, and then click *Session Monitor*.  
Current sessions appear in the right pane.
- 2. Set the Trace Control option for the chosen session to Details.  
Information icons now appear in the Trace FEX column.
- 3. If necessary, run a request for logging, then return to the Administration Console.
- 4. Click the *View Trace* icon .

The Session Viewer appears, as shown in the following image.



- 5. Click a *Zip Session Trace* link and save the zip file.

6. Close the Session Viewer and return to the Session Monitor pane.
7. Set Trace Control to its previous value. Typically, this is OFF.

In response, a message above the Session Monitor table confirms that tracing has been changed or stopped.

## Viewing Sessions

The Session Viewer enables you to review traces of system events that took place during recent work sessions and export them to system administrators or customer support staff. Traces of system events and error messages captured by the Session Viewer provide a clear picture of system operations, and enable you to investigate the causes of system disruptions or performance issues.

The Session Viewer complements the Session Monitor page by extending the range of sessions under review, from those that are currently active, to those that occurred in the past. The parameter Days Until Traces Are Deleted (IBI\_TRACE\_RETAIN\_DAYS) defines the number of days that the Session Viewer retains information about sessions. It also focuses your review by limiting the range of available sessions to those created by you and by those users whose session activities you have permission to review.

You can open the Session Viewer only if you have been assigned the opDevTraces (Development Traces) privilege. This privilege allows you to view traces from your current and previous work sessions. With this privilege, you can open the Session Viewer. To do so, open the *Tools* menu and select *View Sessions*. , From the 8207.27 Home Page, select *Utilities*, and *Session Viewer*.

If you sign in as an administrator, you can view your sessions and sessions for other users. If you sign in as a different user, you can only view sessions made available to you by the opDevTraces (Development Traces) privilege.

## Reviewing the Session Viewer Main Page

The main page of the Session Viewer displays information about your current work session. It also lists entries for all of the recently completed sessions that you have permission to review, as shown in the following image.

The screenshot displays the TIBCO Session Viewer interface. At the top, it shows the session ID 'admin Session Viewer admin\_155454 (211229)'. Below this is a table of sessions. The table has columns: User, Name, File, Tracing Level, SQL Tracing, Grouping, SQL Error, Session Started, Last Activity, URL, Average Response, Server Requests, Average Server Time, and Average DBMS Time. The table lists several sessions for user 'admin' with session IDs like '155454 (211229)'. Below the table, there are tabs for 'Details', 'ZIP Session Traces', and 'Download'. The 'Details' tab is active, showing a list of SQL statements and their execution details for the selected session.

To open the main page of the Session Viewer, sign in as a user who maintains the opDevTraces (Development Traces) privilege. From the Hub, select **Tools** and **View Sessions**. From the WebFOCUS Home Page, select **Utilities**, and **Session Viewer**. The session ID follows the format *username\_HHMMSS* (YYMMDD). It contains the username, starting time, and date of the session on display. For each session, the following information is available:

### User Name

The name of the user that signed in to this work session.

### Viewing File

The name of the Viewing File. File names are identified by their start time and end time in HH.MM format. If an asterisk (\*) is displayed as the end time, current traces are being routed to that file.

You can click **New File**, to capture a new set of traces, which allows users to capture a set of URLs that will be reviewed. When you click this link, the Session Viewer automatically creates a new file and assigns all subsequent traces to it. You can review prior traces by clicking a file containing completed traces in the Viewing File list.

### Tracing Level

The level of traces captured by the current session. The default value for this field is Off, but you can choose another value from the list. The Session Viewer saves this selection when you close the viewer, and uses it as the default setting for your next session.

The four tracing levels are cumulative, meaning each higher level includes the traces of all of the levels below it. These levels include:

- ☐ **Basic.** Generates a trace for each URL, which includes IBFS traces and procedure traces.
- ☐ **Outputs.** Includes Basic level traces and output from URLs that run requests on the Reporting Server. This level of tracing affects the amount of disk space required to capture output traces, but does not affect system performance.
- ☐ **Debug.** Includes Outputs level traces, and log4j debug level written to the Session Viewer output.
- ☐ **Details.** Includes Debug level traces and legacy WFServlet traces. This level of tracing affects session performance.
- ☐ **Server.** Includes Details level traces and generates traces for the Reporting Server activity for the current work session.

### Fex Echo Setting

The level of echo traces captured from the execution of FEX file commands. In a FEX file, the &ECHO variable displays command lines as they execute in order to test and debug procedures. These levels include:

- ☐ **Off.** Suppresses the display of both stacked commands and Dialogue Manager commands in its traces. This value is the default.
- ☐ **On.** Displays TIBCO WebFOCUS commands that are expanded and stacked for execution in its traces.
- ☐ **All.** Displays Dialogue Manager commands and TIBCO WebFOCUS commands that are expanded and stacked for execution in its traces.

### SQL Tracing

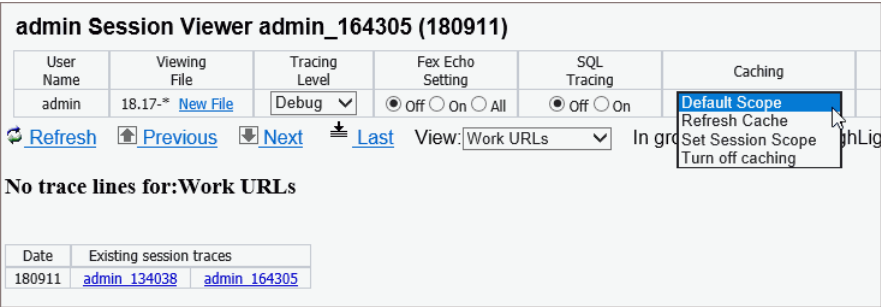
The level of traces captured from SQL events. These levels include:

- ☐ **Off.** Suppresses the display of traces of SQL request and response events.
- ☐ **On.** Displays traces of all SQL request and response events. Even if you select this setting, however, the Session Viewer will not display SQL event traces if there are no requests issued to an SQL database.



Caching

The Caching configuration for the current session. Options in this list override the default caching configuration that is defined on the Application Caches page of the Administration Console Configuration tab, as shown in the following image.



The options in this list affect caching operations for the current session only. They enable administrators and developers to temporarily suspend caching for application development sessions.

When the next session starts, the Default Scope option is automatically reassigned to the list. This option resets the cache to a persistent status for the new session, making it ready for use in a production session.

The list contains the following options.

Default Scope

When this option, also known as the User Scope, is selected, data source values remain in the cache and Lru Cache statistics are not cleared when a session ends. This is the default option for the Caching list. It allows cached data and cache statistics to persist from session to session.

This option displays the Default Scope label when it is selected and the Set Default Scope label when it is not selected.

Session Scope

Displays the Session Scope label when it is selected and the Set Session Scope label when cleared.

No Caching

Suspends caching in the current session. After you select this option caching is suspended within the session until you select Set Session Scope or Set Default Scope. This option displays the No Caching label when it is selected and the Turn Off Caching label when cleared.

**Refresh Cache**

Refreshes the cache and immediately restores the option that was previously selected.

**JS Error Popup**

Activates the capture of JS Error Popup messages in the session trace. The On option is selected, by default, indicating that JS Error Popup messages are included in the Session Trace.

**Session Started**

The time that your active session started, in HH.MM.SS format.

**Last Activity**

The start time of the most recent activity in your active session, in HH.MM.SS format.

**URL Count**

The total number of URLs issued for the session that you are viewing.

**Average Response**

The average response time, in seconds, for all URLs issued for the session that you are viewing.

**Server Requests**

The number of requests made to your Reporting Server during your active session.

**Average Server Time**

The average time (in seconds) that it takes the Reporting Server to respond to a request.

**Average DBMS Time**

The average time (in seconds) that it takes the Reporting Server to respond to a request directed to a non-TIBCO WebFOCUS or RDBMS database.

If no current session file is available, the section below the status bar displays the following text:

`Session file does not exist.`

If a current session file is available, the section below the status bar lists traces for that file.

If you are signed in as an administrator, you can also view a table containing links representing recently completed sessions. If multiple viewable sessions occurred on a specific date, they are listed from left to right in that table in the order in which they occurred, earliest to latest.

Information from completed sessions remains available for the period defined in the setting, Days Until Traces Are Deleted (IBI\_TRACE\_RETAIN\_DAYS).

To view a different session, click a session link on the main page or the session details page. A new page displaying traces for your selected session opens.

**Note:** The session information links connect to completed sessions only. To view a current session, open the Session Monitor page from the Administration Console, and click an Information icon, if one appears.

Reviewing the Session Details Page

To open the session details page, click a session link in the Existing session traces column of the main page. The session details page opens, as shown in the following image:



This page displays a group of features that enables you to review relevant details about your selected session, review summary versions of the traces it created, and move on to other sessions.

When the review of your selected session is complete, close the session details page to return to the main page.

When you open the session details page, your sign-in information and the ID of your selected session appear at the top of the screen.

A table underneath the Session ID lists additional details identifying the session under review. The User Name entry identifies the name of the user who initiated the session on display.

The Viewing File entry identifies the range of trace entries on display, as defined by start time. By default, this value displays the entire range of trace entries from the start time to an undefined end time. If a drop-down button appears, you can select a different time range from the drop-down menu.


You can use the following options to change the display of trace information that you want to view.

- ☐ **Refresh.** Adds any traces to the list that were generated after you opened an active session. This option is not available to previously completed sessions.
- ☐ **Previous.** Moves the display back to view an earlier set of traces.
- ☐ **Next.** Moves the display forward to view a later set of traces.
- ☐ **Last.** Moves the display to view the final set of traces captured right before the end of the session.
- ☐ **View.** Limits the list of traces by type.
  - ☐ **All URLs.** Displays URLs that return static content, such as .css files, .html files, .js files, and dynamic URLs that perform a Client action, as well as URLs that perform an action on the Reporting Server.
  - ☐ **Work URLs.** Limits the display to dynamic URLs, as well as Reporting Server requests. This is the default setting.
  - ☐ **Server Requests.** Limits the display to URLs that access the Reporting Server.
- ☐ **In groups of.** Determines the number of trace entries that appear on a single page. You can select 1, 5, 10, 25, 50, 100, or 200. Your selection in this field impacts the use of the Previous, Next, and Last options. The larger the value you select, the fewer times you will be required to move to the previous or next page.
- ☐ **HighLight.** Assigns a yellow highlight to the start time field of all trace entries that contain the search term that you type in this field.

For example, if you type the term *short*, a highlight appears in the Start Time field for any trace entry that contains this term, such as:

```
IBFS checkPolicy Success  
IBFS:/EDA/ACTWIN7/ibisamp/short.mas
```

**Note:** To clear the highlights, delete the value from the Highlight field, and then press the Enter key.

-  **ZIP Session Traces.** Saves all of the traces from the session to a single zip file. When you click this link, you are prompted to open or save the file. Click Save As, browse to a storage location for the zip file, and then click Save.

The default name for this zip file is the user name, followed by the number of trace and log files it contains. For example, admin\_140841.

These options also appear below the trace information table.

**Note:** If you select two time bars, the page refreshes and displays a timeline between the two transactions they represent, as shown in the following image.



The screenshot displays the TIBCO Session Viewer interface for session admin\_154229 (211229). The top navigation bar includes buttons for 'Previous', 'Next', and 'Last'. Below the navigation bar is a table of session events with columns for 'Time', 'Event', and 'Details'. The table shows a sequence of events from 15:01:00 to 15:01:40. A timeline bar at the bottom allows selecting two time bars to view the timeline between those transactions. The interface also includes a search bar and a 'ZIP Session Traces' button.

When your review is complete, select one of the two time bars to return to the default view.

The trace information table enables you to review individual session traces in more detail. It displays one summary entry for each trace captured during the session. You can expand these entries to review the detailed event messages captured by the trace.

The table located below the trace information table and options identifies the User Agent and Build that started the session. Details identifying the User Agent include the browser, operating systems, and supporting applications. Details identifying the Build include, the version number, build number, and generation date of the product version to which this session was connected.

A list of recently completed sessions appears at the bottom of the page. This list is a duplicate of the session list on the main page and appears here to enable you to move on to another session without having to leave the session details page.

## Reviewing Trace Entries

Each entry in the list of traces on the session details page represents the record for a single system activity, as shown in the following image.

Start	End	1.28 Max	
11:45:38	11:45:39		@ Id:URL823 AD Drill//contentDrill.vxl?value_0=United States&valueft_0=United States&dmVerKeyName=fdmId_3_15bc4b00141&eddata=YW19QjZjZ2lkPkhQVlUumY38pZD1

One activity can include multiple events, and these events become visible when you expand the icon next to a trace to view its full detail.

For each trace, the following information is available:

### Start

The time, in hours, minutes, and seconds, that an event in the trace began. Hours are expressed in twenty-four hour time notation.

### End

The time, in hours, minutes, and seconds, that an event in the trace ended. Hours are expressed in twenty-four hour time notation.

### Number of Seconds Max

The number in the header of this column represents the maximum number of seconds that were required to complete the longest trace in the list.

Entries in this column contain a (time) bar that represents the relative duration of the events in the trace, as shown in the following image.



- ☐ The darkest blue section of the bar represents the number of Web CPU seconds that were required to process the events in this trace. It also identifies the trace as containing a Work URL component.
- ☐ The black section of the bar represents the number of Web wait seconds that were required to retrieve a response from a database. It also identifies the trace as containing a Work URL component.
- ☐ The brown section of the bar represents the number of Reporting Server seconds that were required to process the events represented in this trace. It also identifies the trace as containing a Server Request component.

You can view tooltips that identify the exact number of seconds that each section of a bar represents by pointing to that section with your mouse. If you are reviewing an active trace in a current session, the bar appears green and occupies the entire column entry. If you hover the mouse over the bar, a tooltip that contains the number of seconds that have already elapsed during that event appears.

### Details

The ID of the trace. This is the URL of the destination of the request message that launched the trace events. The first term in the URL identifies the servlet or other application that launched the request. Each trace ID is unique.

When the URL ID number is highlighted in orange, events in the trace associated with it include one or more error messages. Within the detail trace display, events that contain error messages are also highlighted in orange to help you identify when the errors occurred.

### Reviewing Expanded URL Details

When you expand an individual Trace Details list entry, a nested list of system-generated messages opens. These messages identify the events captured by that trace and the time, in milliseconds, at which those events took place. Events include request and response messages exchanged between the Client and the Reporting Server or between the Reporting Server and the application server. They also include error messages, informational messages, and system status messages generated by application programs as they execute commands. Entries representing repetitive or subordinate events are nested to help you identify them more quickly, as shown in the following image.

```

55 INFO IBFS+ { Start:IBFSService.getItem
55 INFO IBFS+ { Start:IBFSServiceInt.pr
56 DEBUG IBFS Setting Session variables into
57 DEBUG IBREPOSITORY IBI_INFOSEARCH_ENGINE:
58 INFO IBFS prepareArgs REQ_PERMS:
58 DEBUG IBFS fetchCachedSecInfo Security use
58 INFO IBFS checkPolicy Success IBF
58 INFO IBFS- } End:IBFSServiceInt.prep
59 DEBUG IBFS Setting Session variables into
59 INFO IBFS MRE.getItem path:IBFS:/WFO
60 INFO IBFS MRE.getItem got:class com.
60 INFO IBFS checkPolicy Success IBFS:/
60 INFO IBFS- } End:IBFSService.getItem re

```

A trace entry begins with the event start time and the number of milliseconds after the trace start time at which the event took place. This value helps you distinguish between individual events, and places them in sequence within an individual trace.

The IBFS status code for the trace event follows the event start time.

This column contains one of the following symbols:

Symbol	Description
IBFS+	The starting event of a program or exchange of data between programs or applications.
IBFS-	The ending or final event of a program or exchange of data between programs or applications.
IBFX*	An error message.
IBFSX	An administrative or informational message.

The text of the message generated by the application or program that describes the event appears next. The type of text displayed in this section varies with the type of trace you have selected from the View drop-down list.

- ☐ If you select *All URLs* or *Work URLs*, an expanded URL entry displays the status and error messages that were generated as the program ran.

**Note:** If your entry includes a Server Request message, the underlined Request ID term of the trace entry links you to full details of the Reporting Server Request trace, and the underlined Response ID entry links you to full details of the Reporting Server Response trace.

- ☐ If you select *Server Request*, an expanded URL entry displays the Reporting Server Request procedure, followed by a list of status or error messages generated during that procedure. (This is the same display that appears when you open a Server Request link from a Session Monitor Information icon.)



## Reviewing Reporting Server Request Details

Traces captured from a Reporting Server Request identify the details of the query or other request operation sent from the Client to the Reporting Server during the session, as shown in the following image.

```
Plain text:---Focexec-Start--- RequestID=URL56Req1 UrlID=URL56 ReqInfo="Run:Domain=Sales/:App=sales:SubAct=MR_STD_REPO
....:SET PCHOLD-FMT=XML
....:*WF
....:GKE %MRE USERID admin
....:GKE %MRE DOMAIN Sales/
....:GKE %MRE BASEDIR IBFS:/WFC/Repository/Sales
....:GKE %MRE APPDIR sales
....:GKE %MF FEXNAME cost_of_goods_ytd
....:GKE %MF FULLFEXNAME Cost of Goods YTD
....:GKE %IP 10.98.96.234
....:
0001:EX -LINES 6 EDAPUT FOCEXEC,mrheader,C,MEM,-* mr header include start
0002:-* mr as NOT html
0003:-SET &FOCEXURL-&FOCEXURL | 'IBIMR_drill=IBFS,RUNFEX,IBIF_ex,true' | '&';
0004:SET FOCEXURL='&FOCEXURL'
0005:-* mr header include end
0006:-*
0001:EX -LINES 47 EDAPUT FOCEXEC,cost_of_goods_ytd,C,MEM,ENGINE INT CACHE SET ON
0002:SET PAGE-NUM=NOLEAD
0003:SET SQUEEZE=ON
0004:-DEFAULTH &WF_HTMLENCODING=ON;
0005:SET HTMLENCODING=&WF_HTMLENCODING
0006:-*
0007:SET HTMLCSS=ON
0008:-DEFAULTH &WF_EMPTYREPORT=ON;
0009:SET EMPTYREPORT=&WF_EMPTYREPORT
0010:-*
0011:SET EMBEDHEADING=ON
0012:SET GRAPHDEFAULT=OFF
0013:SET COMPONENT=TableChart_1
0014:SET ARVERSION=2
0015:-DEFAULTH &WF_TITLE='WebFOCUS Report';
0016:GRAPH FILE retail_samples/wf_retail_lite
0017:-* Created by Designer for Graph
0018:SUM WF_RETAIL_LITE.WF_RETAIL_SALES.COGS_US
0019:BY WF_RETAIL_LITE.WF_RETAIL_TIME_SALES.TIME_YEAR
0020:ON GRAPH PCHOLD FORMAT JSCHART
0021:ON GRAPH SET VZERO OFF
0022:ON GRAPH SET HAXIS 770.0
0023:ON GRAPH SET VAXIS 405.0
0024:ON GRAPH SET LOOKGRAPH LINE
0025:ON GRAPH SET EMBEDHEADING ON
0026:ON GRAPH SET AUTOFIT ON
0027:ON GRAPH SET STYLE *
0028:*GRAPH_JS
0029:  "injectedRevision" : "$Revision: 1.2 $",
0030:  "dataSetLimits": {"enabled": true},
0031:  "catchErrors" : true
0032:*END
0033:-INCLUDE _c/theme
0034:TYPE=REPORT, TITLETEXT='Chart1', ARREPORTSIZE=DIMENSION, ARFILTER_TARGET='*', ARGRAPHENGINE=JSCHART, $
0035:TYPE=DATA, COLUMN=N1, BUCKET=x-axis, $
0036:TYPE=DATA, COLUMN=N2, BUCKET=y-axis(1), $
0037:*GRAPH_SCRIPT
0038:-*
0039:*GRAPH_JS_FINAL
0040:"blaProperties": {
0041:"seriesLayout": "absolute"
0042:}
0043:-*
0044:*END
0045:ENDSTYLE
0046:END
```

This information identifies the variables and commands sent during the request operation. These requests are usually TABLE requests or -HTMLFORM BEGIN/END requests that are sent from the Client to the Reporting Server.

The ID term in the first line above the procedure links it to the URL trace from which it was generated. For example: the ID, *URL 101*, links the procedure to the server request event line within the activity captured in trace URL 101.

At the end of the list of variables and commands, the procedure displays a list of status messages describing the results of the query or other operation, as shown in the following image.

```
.....SET PCHOLD-FMT=BINARY
-----End----- RequestID=URL170Req12 UrlID=URL170 ReqInfo="Run:Domain=Public/:SubAct=MR_STD_REPORT:Fex=WebFOCUS_Report" Lines=651
---Server-Report--- RequestID= URL170Req12 ReportID= URL170Req12Rep Mime= .HTML OutputSizeK= 2 OutputLines= 4 File= URL170Req12Rep.htm N
---Message-Start--- RequestID=URL170Req12 UrlID=URL170 ReqInfo="Run:Domain=Public/:SubAct=MR_STD_REPORT:Fex=WebFOCUS_Report" FocMsgs=0
.....:0 NUMBER OF RECORDS IN TABLE= 10 LINES= 10
.....:0 HOLDING HTML FILE ON PC DISK ...
-----End----- RequestID=URL170Req12 UrlID=URL170 ReqInfo="Run:Domain=Public/:SubAct=MR_STD_REPORT:Fex=WebFOCUS_Report" FocMsgs=0
---Server--Times--- RequestID=URL170Req12 UrlID=URL170 ReqInfo="Run:Domain=Public/:SubAct=MR_STD_REPORT:Fex=WebFOCUS_Report" Reports=1
```

## Reviewing Reporting Server Response Details

Traces captured from a Reporting Server response identify the information returned in response to a query or other request operation sent from the Reporting Server to the Client during a work session.

To view output traces, click on the link from an underlined URL request response entry in a URL Trace entry, such as:

[URL103Req4Resp](#)

The first part of this display identifies the format variables returned to the Client during the response operation, as shown in the following image.

```
<!DOCTYPE html>
<html>
<head>
<meta name="HandheldFriendly" content="True">
<meta name="PalmComputingPlatform" content="True">
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=5, user-scalable=1"><title>Report1</title>
<script type="text/javascript">
</script>
<style type="text/css">
#IBI_popupHere { position:absolute; visibility:hidden; z-index:200; }
</style>
<script language="javascript">
var ibiOptions = new Array("popupdesc");
var focxurl = "/ibi_apps/WFServlet?IBIF_id=ibi_apps&IBIC_server=EDASERVE&IBIAPP_app=sales&IBIMR_drill=IBF5, RUNFEX, IBIF_ex, true&";
var fochtmlurl = "/ibi_apps/ibi.html";
var serverLanguage='en';
</script>
<script language="javascript" src="/ibi_apps/ibi_html/javaassist/nls.js"></script>
<script language="javascript" src="/ibi_apps/ibi_html/javaassist/ibi/html/js/ibighl.js"></script>
<style type="text/css">
<!--
TABLE { border-collapse:collapse; }
BODY { background-color:#FFFFFF; }
TD { vertical-align:top; padding-left:6pt; padding-right:6pt; }
.X7 { font-family:ARIAL; font-size:9pt; font-weight:normal; font-style:normal; text-decoration:none; color:#141414;
border-top: 1.00pt SOLID #0B0B0B; border-bottom: NONE; border-right: NONE; border-left: NONE; }
.X6 { font-family:ARIAL; font-size:9pt; font-weight:normal; font-style:normal; text-decoration:none; color:#141414; padding-top:3pt; padding-bottom:3pt;
border-style: NONE; }
.X4 { font-family:ARIAL; font-size:9pt; font-weight:normal; font-style:normal; text-decoration:none; color:#141414; padding-top:3pt; padding-bottom:3pt;
border-top: 1.00pt SOLID #0B0B0B; border-bottom: NONE; border-right: NONE; border-left: NONE; }
.X5 { font-family:ARIAL; font-size:9pt; font-weight:normal; font-style:normal; text-decoration:none; color:#141414; padding-top:3pt; padding-bottom:3pt;
border-top: 1.00pt SOLID #0B0B0B; border-bottom: NONE; border-right: NONE; border-left: NONE; }
.X2 { font-family:ARIAL; font-size:9pt; font-weight:bold; color:#141414;
border-style: NONE; }
.X3 { font-family:ARIAL; font-size:9pt; font-weight:bold; color:#141414;
border-style: NONE; }
-->
</style>
<script language="javascript">
ibighlloadCss(null);
</script>
</head>
```

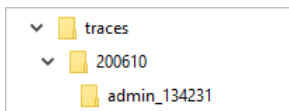
The second part of the display identifies the data returned to the Client during the response operation, as shown in the following image.

```
<tr>
<td style="vertical-align:bottom" class="x2">
COUNTRY</td>
<td style="vertical-align:bottom" class="x3">
CAR</td>
</tr>
<tr>
<td class="x4">
ENGLAND</td>
<td class="x5">
JAGUAR</td>
</tr>
<tr>
<td class="x6">
</td>
<td class="x5">
JENSEN</td>
</tr>
<tr>
<td class="x6">
</td>
<td class="x5">
TRIUMPH</td>
</tr>
<tr>
<td class="x4">
FRANCE</td>
<td class="x5">
PEUGEOT</td>
</tr>
<tr>
<td class="x4">
ITALY</td>
<td class="x5">
ALFA ROMEO</td>
</tr>
<tr>
<td class="x6">
</td>
<td class="x5">
MASERATI</td>
</tr>
```

By default, the Session Viewer displays the report itself when you click on the link, `URL###Req##Rep`. To view the results in HTML format, save the file as a text file, and reopen it. Reporting Server responses usually contain data or status messages returned in response to SQL-based queries, updates, or other database-related operations.

## Saving Trace Files

The Session Viewer retains trace information in a set of files stored in the *traces* directory located at `drive:\ibi\WebFOCUS_WFI\WebFOCUS\traces` in Windows or `install_directory/ibi/WebFOCUS_WFI/WebFOCUS/traces` in UNIX or Linux, as shown in the following image.



Within this directory, there is one daily session activity folder for each day on which user sessions took place within the period defined by the Days Until Traces Are Deleted (IBI\_TRACE\_RETAIN\_DAYS) setting. To make them easily identifiable, these folders use the date on which they were created, in the format YYMMDD, as their title.

Within a daily session activity folder, there is one folder for each session that took place on that day. This folder contains all files created during that session, and the name of the folder is a shortened version of the session ID.

The automated capture and filing of session records makes it easy to find sessions from prior days while keeping your system resources free of excess trace records. The use of a date as the title of the folder containing all sessions for a single day enables the daily sweep for outdated trace files to identify those folders that have exceeded their maximum retention period and are ready to be removed.

If you must save session traces that will not be deleted by this automated sweep, you must create a separate folder within the traces directory and use a name such as *save* or some other readily identifiable term that does not use the YYMMDD format. You must then capture a zipped copy of the session trace files and save them to this separate folder manually. These files will be available for review until you delete them yourself.

### Session Folder Contents

A session folder contains the session.log file and the procedure.log file, along with the .trace file, .dat file, .header file, and .xml file for the URLs that were called during the session.

- ☐ The .traces file contains records of system events captured during the call to or from the URL.
- ☐ The .dat file contains the .html data that defined in the URL call.
- ☐ The .header file contains data included in the header of the message that was a call to or from the URL.
- ☐ The .xml file contains all relevant parameters involved in the call.

The detailed records within these files are described in the previous topics within this section.

### ***Procedure:*** How to Export Session Viewer Trace Files

Ensure that a folder with a name that does not use the date format YYMMDD has been created in the *traces* folder, located at *drive:\ibi\WebFOCUS\_WFI\WebFOCUS\traces* for Windows or *install\_directory/ibi/WebFOCUS\_WFI/WebFOCUS/traces* for UNIX or Linux. If no such folder appears, create it before implementing this procedure.

1. Open the Session Viewer.
2. Select the *Zip Session Trace* link to save the current session.

Or

In the list of sessions beneath the current session table, click the link to a previous session and then click the *Zip Session Trace* link to save it.

3. When your browser prompts you to open or save the file, select *Save As*.

4. Navigate to the following location for the trace file:

*drive:\ibi\WebFOCUS\_WFI\WebFOCUS\traces\undatedfolder\username\_time\*

if you are using Windows

Or

*install\_directory/ibi/WebFOCUS\_WFI/WebFOCUS/traces/undatedfolder/  
sessionID*

if you are using Unix or Linux.

Where:

*undatedfolder*

Is the name of the folder that contains zipped session files that must be retained beyond the number of days specified in the Days Until Traces Are Deleted (IBI\_TRACE\_RETAIN\_DAYS) parameter. This name must not use the date format YYMMDD.

*sessionID*

Is the unique ID assigned to the session. It combines the name of the user who opened the session with the time of day on which the session occurred, separated by an underscore.

5. Confirm that the zip file was saved in the targeted location and close the Session Viewer.

## Working With Log Files

The Log Files page displays links to all log files in a single location, where you can review or capture copies of them instantaneously when required to provide records of system events to the Customer Support Team to support troubleshooting or system analysis in response to production issues.

The main grid lists log files, in alphabetical order, by name. Next to each Log Name entry is a list of Logger Names, that is, those pages or events that contribute entries to that log. For example, the audit.log file captures events from com.ibi.uoa, com.ibi.config, com.ibi.content, and others.

Log files contain records of system events. The Log Level field, next to each Logger, identifies the level of events captured by that contributor.

Log levels are cumulative. Events captured by a higher level are included when you select a lower level. For example, if you set the level to **WARN**, you will capture **FATAL** level and **ERROR** level events, as well as events that generate a warning.

The levels are defined below:

- ☐ **OFF.** Capture no events.
- ☐ **FATAL.** Capture only events that disrupt system operations.
- ☐ **ERROR.** Capture events that generate error messages in addition to fatal events.
- ☐ **WARN.** Capture events that generate warning messages in addition to fatal and error events.
- ☐ **INFO.** Capture events that generate informational messages in addition to warning, error, and fatal events.
- ☐ **DEBUG.** Capture events that generate debug messages in addition to informational, warning, error, and fatal events.
- ☐ **TRACE.** Capture events that generate trace messages in addition to debug, informational, warning, error, and fatal events.

For more information about the log and trace files and events they capture see [Logging](#) on page 591.

The log levels assigned to the audit log files are preset, and are not available for updates. You can adjust the log level assigned to any of the other log files. However, when you recycle the application server, all log levels revert to their default value.

To help you identify problem conditions quickly and easily, log entries for WARN, ERROR, and FATAL events are highlighted as follows:

- ☐ **WARN.** Yellow
- ☐ **ERROR.** Orange
- ☐ **FATAL.** Coral

Color-coded highlights support reviews and troubleshooting by distinguishing log entries of events capturing errors or problem conditions from those capturing routine system events. The use of a consistent color for each of the three event categories helps narrow the search for problem events of a specific level of severity.

Because these highlights are applied by the log file viewer, they appear only when you open and review log files from the Log Files page. Highlights are not saved in zipped copies of the log files, and they do not appear when you open and review log files in a different text editor.

The *Zip All* button saves copies of all log files and the systeminfo.xml file into a single zip file. You can use this button to capture records of system events and system information whenever necessary.

The *Reset All to default* button restores the default log levels to all settings that allow you to adjust the logging level.

The log files include records of events from the start of the current day until the time you create the zip file. Event records captured in the log files support troubleshooting and analysis.

The `systeminfo.xml` file contains a snapshot of the values assigned to system information settings at the time you create the file, including JVM Property Information page values, Application Setting page values, and License Information. The `info-date` tag at the beginning of the file records the date and time at which the file was created and the values in it were captured.

**Note:** The Log Files page does not display Web Services traces or client traces. To view these traces, open the Session Viewer or the Session Monitor. For more information about these two features, see [Viewing Sessions](#) on page 186 or [Monitoring Sessions](#) on page 183.

## Working With Log Pages

Log pages list detailed records of system events that were captured in a log file in order of the time of their occurrence, from the earliest event on the day of the log to the most recent.

To open a log file for review, click a link from the Log Name column on the Log Files page. The page for your selected log file opens in a separate window.

The name of the log file appears at the top of the page. A list of earlier versions of that log file also appears at the top of the page. This list contains all previous versions of that log file that are currently available in the `drive:\ibi\WebFOCUS82\logs` directory. The number of days to retain a log file is defined in the setting Days Until Logs Are Deleted (`IBI_LOG_RETAIN_DAYS`) found on the Application Directories page of the Configuration tab of the Administration Console.

The *New trace lines* link appears beneath the file name. Click this link to refresh the log page with entries for system events that occur after you open it. New records are posted to a log file automatically. To protect the integrity of this information, no one can use a log page to update or change log file records.

The *Bottom* link takes you directly to the last entry in the file. This link is useful when you must review a file with a large number of entries, and you want to move directly to the most recent event. Similarly, the *Top* link, that appears below the last entry, returns you to the first entry in the log file and the features that appear on the top of the page.

The list of individual event entries begins below the Bottom link. Individual entries start with the date and time, in hours, minutes, seconds, and milliseconds, that an event took place. A code name identifying the category of event and the specific event itself follows the date and time. A full description of the event comes next. This description includes any messages generated by the system in response to the event.

You can use the log page to review and search for records of specific events in response to a query from a customer service support team member. The Find command in your browser can help you search for an event by a unique message, event name, or timestamp. You can also scroll through records to locate an event.

When your review is complete, close the log page window. You can use the Save or Print command in your browser to save or print a copy of the log page, or you can capture a zipped copy of it using the Zip All button from the Log Files page.

## Working With Application Log Files

The Application Log Files page displays links to all log files generated from application utilities, as shown in the following image.

Configuration Security ReportCaster Diagnostics			
Diagnostics			
<ul style="list-style-type: none"> <li>▼ Diagnostics           <ul style="list-style-type: none"> <li>About TIBCO WebFOCUS</li> <li>Client Verification</li> <li>HTTP Request Info</li> <li>JVM Property Info</li> <li>Session Monitor</li> <li>Log Files</li> <li><b>Application Log Files</b></li> <li>Lru Cache Statistics</li> </ul> </li> </ul>			
Application Log Files			
Log Name		Log Size	Log Date
<a href="#">cm_import_bip_page_templates_v03_2021-12-28_12-50-31.log</a>		4087153	2021-12-28 12:50:41
<a href="#">cm_import_junit_healthnet_db_v1_2021-12-28_12-56-21.log</a>		22547295	2021-12-28 12:56:47
<a href="#">cm_import_junit_healthnet_v1_2021-12-28_12-56-09.log</a>		908123	2021-12-28 12:56:21
<a href="#">cm_import_managers_group_and_rules_2021-12-28_12-50-24.log</a>		1305230	2021-12-28 12:50:31
<a href="#">cm_import_my_workspace_v01_2021-12-28_12-50-58.log</a>		1275467	2021-12-28 12:51:05
<a href="#">cm_import_P215_S20063_2021-12-28_12-56-01.log</a>		671720	2021-12-28 12:56:09
<a href="#">cm_import_P215_S29948_2021-12-28_12-56-54.log</a>		657680	2021-12-28 12:57:01
<a href="#">cm_import_P23_S29954_2021-12-28_12-56-48.log</a>		648240	2021-12-28 12:56:54
<a href="#">cm_import_PDfiles_HEAD_2021-12-28_12-57-24.log</a>		900825	2021-12-28 12:57:34
<a href="#">cm_import_pgx_page_templates_v05_2021-12-28_12-50-41.log</a>		2223415	2021-12-28 12:50:51
<a href="#">cm_import_Retail_Samples_Domain_CM_v08_2021-12-28_12-59-47.log</a>		1399484	2021-12-28 01:00:03
<a href="#">cm_import_roles_2021-12-28_12-50-17.log</a>		1515068	2021-12-28 12:50:24
<a href="#">cm_import_Testing_Performance_Portal_2021-12-28_12-57-12.log</a>		1012354	2021-12-28 12:57:24
<a href="#">cm_import_themes_v05_2021-12-28_12-50-51.log</a>		1348447	2021-12-28 12:50:58
<a href="#">cm_import_WFPMResponsiveDemo_2021-12-28_12-57-01.log</a>		900086	2021-12-28 12:57:12
<a href="#">WFReposUtilCMDLine_2021-12-28_12-50-06.log</a>		591293	2021-12-28 12:50:16



The Application Log Files page displays links to all log files generated from application utilities. Using this page, you can review application log files, and the records they contain, when you need to analyze errors or production issues that occurred when running an application utility. By making it easy to find and review application log information, the Application Log Files page saves you time when troubleshooting the operation of a standalone utility, such as a change management import or export. This page supports your efforts to quickly resolve any issues you may encounter, and provides you with a way to share records of utility operations with the Customer Service team.

The main grid lists application log files by name. Typically, the Log Name entry contains the name of the application utility that generated the log and the date and time at which the utility that created the log was run.

For example, the `cm_import_bip_page_templates_v03_2018-06-06_23-50-51.log` file captures events from the change management import of the BIP Page templates CM package that took place on June 6, 2018. However, the value assigned to a Log Name entry depends upon the data and format selected by the utility that creates it, and the information and format of individual log names may vary as a result.

The Log Size entry identifies the size, in kilobytes, of the log file, and the Log Date identifies the date and time the application log file was created in YYYY-MM-DD HH:MM:SS format.

Logs that appear on this page are generated by utilities that appear in the system folder:

`drive:\ibi\WebFOCUS82\utilities`

These utilities accomplish such tasks as change management imports or database updates. A standard set of these utilities is loaded into this folder during product installation. However, logs created by other utilities that are added to this folder after installation can also appear on the Application Log Files page.

The application logs themselves are stored in the system folder:

`drive:\ibi\WebFOCUS82\application_log`

The number of days to retain an application log file is defined in the Days Until Logs Are Deleted (IBI\_LOG\_RETAIN\_DAYS) setting, which is located on the Application Directories page of the Administration Console Configuration tab.

## Working With Application Log Pages

Application log pages list detailed records of system events that occurred during the execution of an application utility. Events are listed in the order of the time of their occurrence, from the earliest event to the final event. You can use the application log page to review and search for records of specific events.

To open an application log page for review, click a link from the Log Name column on the Application Log Files page. Your selected application log file page opens in a separate window.

The name of the log file appears at the top of the page. The Bottom link takes you directly to the last entry in the file. This link is useful when you must review a file with a large number of entries, and you want to move directly to the most recent event at the end of the log. Similarly, the Top link appears below the last log entry. It returns you to the first and earliest entry in the log file.

The list of individual events begins after the Bottom link. Typically, individual entries start with the date and time, in hours, minutes, seconds, and milliseconds, that an event took place. A code name identifying the category of event and the specific event itself follows the date and time. A full description of the event comes next. This description includes any messages generated by the system in response to the event. Some utilities, especially those from third parties or those added after the installation, may not generate entries that follow this pattern.

When your review is complete, close the application log page window. You can use the Save or Print command in your browser to save or print a copy of the application log page.

## Working With LRU Cache Statistics

The Lru Cache Statistics page displays current cache usage statistics, as shown in the following image.

Lru Cache Statistics										
Cache Name	Max Memory(K)	Current Entries	Current Memory(K)	Gets No-Hit	Gets Hit	Put Obj Count	Remove Obj Count	LruPrune Entries	LruPrune Memory	Clear Count
MetaData	50000	0	0	76	94	148	66	0	0	19
DataValues	50000	3	54	51	0	3	0	0	0	19
Group by <a href="#">Scope</a> <a href="#">Path</a> <a href="#">User</a>						Count	MemoryK	Oldest Age	Last Ref	
User						3	54	389s	388s	
ServerConfig	0	0	0	0	0	0	0	0	0	19

This page gives you an overview of the current amount of resources allocated to each cache, the number of entries they contain, the memory allocated to them, and the number of objects or events that added data to the cache, retrieved data from it, cleared data from it, or removed old and unused data from it to make way for new data.

Based on these statistics, you can infer the current status of activity in a cache, determine if metadata or data source values are successfully loading into a cache, identify when a cache is operating at peak capacity, and learn if data or metadata was removed or cleared from the cache.

The name LRU Cache is derived from the fact that all caches follow a Least Recently Used rule. Under this rule, resources that have been unused the longest are the first to be cleared from the cache when the addition of new resources would cause the cache to exceed the amount of memory allocated to it.

To open the LRU Cache Statistics page, open the Administration Console, click the *Diagnostics* tab, and then click *LRU Cache Statistics*.

Values assigned to the statistics on this page result from events that occurred during cache operations, and the layout of entries on this page follows the organization of the individual caches that comprise the total cache allocation within the Application Server memory, and the structure of records within individual caches.

## Understanding the Cache Statistics Page Layout

Entries on the LRU Cache Statistics page are organized by rows, one row per cache, as shown in the following image.

Cache Name	Max Memory(K)	Current Entries	Current Memory(K)	Gets No-Hit	Gets Hit	Put Obj Count	Remove Obj Count	LruPrune Entries	LruPrune Memory	Clear Count
MetaData	50000	0	0	65	27	77	12	0	0	5
DataValues	50000	0	0	0	0	0	0	0	0	5
ServerConfig	0	0	0	0	0	0	0	0	0	5

## Understanding Cache Entries

Entries for the following caches appear on the Lru Cache Statistics page, by default.

### MetaData

This cache captures metadata values produced from calls to the Reporting Server initiated automatically by the client whenever a user selects the Insight mode to run a chart. These calls include requests to the server for information, fonts, and metadata that are shared throughout all Insight Charts. Paths to the resources that place metadata in this cache and the amount of memory to be allocated to this cache are predefined, and the cache is therefore activated automatically as soon as a user chooses to work with a chart in Insight mode. The settings that configure this cache and its operations are pre-configured, and are not available to administrators. If you need to reconfigure or adapt this cache, please contact the Customer Support team.

### **DataValues**

This cache captures data values from queries in user-initiated procedures that create reports, charts, portals, dashboards, and other content. Paths to the resources that place data in this cache are defined in the Data Values Global Cache Paths (IBI\_DATAVALUES\_CACHE\_GLOBALPATHS) setting and in the Data Values User Cache Paths (IBI\_DATAVALUES\_CACHE\_INCLUDEPATHS) setting, located on the Application Caches page of the Administration Console configuration tab.

### **ServerConfig**

This cache captures metadata values used by server operations that are not explicitly related to queries from user-initiated procedures. Paths to the resources that place metadata in this cache and the amount of memory to be allocated to this cache are pre-configured, and are not available to administrators. If you need to reconfigure or adapt this cache, please contact the Customer Support team.

## **Understanding Cache Statistics**

The columns at the top of the page identify the statistics captured for each cache. With the exceptions of Current Entries and Current Memory, these statistics reflect cumulative activity through multiple sessions. They are cleared only when the caches close. The Current Entries and Current Memory statistics are cleared whenever a Clear Cache operation takes place.

For each cache, the following statistics are available:

### **Max Memory (K)**

The maximum amount of memory on the machine hosting the Application Server that is allocated to this cache. For the Data Values Cache, the value in this column is determined by the value assigned to the Data Values Max Cache Memory (MB) (IBI\_DATAVALUES\_CACHE\_MAXMEG) setting for the DataValues row. The maximum amount of memory is pre-configured for the MetaData cache and the ServerConfig cache and is not available to administrators for reconfiguration. Note that the amount of memory allocated to these settings is expressed in megabytes in the Application Caches page setting, but the same amount is expressed in kilobytes in this statistic. Therefore, a value of 50 in the Data Values Max Cache Memory (MB) (IBI\_DATAVALUES\_CACHE\_MAXMEG) setting appears as 50,000 in this entry. This value remains the same throughout a session unless an administrator changes the value in the Data Values Max Cache Memory (MB) (IBI\_DATAVALUES\_CACHE\_MAXMEG) setting.

**Current Entries**

The number of data entries currently held in the cache. Each entry contains the IBFS path to the resource that contains the data retrieved by the query, followed by each individual data source value, the name of the user that ran the procedure that placed data in the cache, and time stamps for the time it was added to the cache and the most recent time it was retrieved for re-use. This value changes as entries are added to, removed from, or cleared from the cache.

**Current Memory (K)**

The current amount of memory that is being used by the data values in the cache. The value in this statistic less the value in the Max Memory (K) statistic identifies the amount of memory available for any additional data. This value changes as data entries are added to, removed from, or cleared from the cache.

**Gets No-Hit**

The number of Get objects that did not successfully retrieve metadata or data values from the cache. This number represents the number of procedures that ran but were unable to retrieve data from the cache because data from the query had not previously been added to it. This value increases whenever a Get object is unable to retrieve data or metadata from the cache. This value does not decrease, and is cumulative across multiple sessions. It returns to zero only when the cache itself is closed.

**Gets Hit**

The number of Get objects that successfully retrieved values from the cache. This number represents the number of procedures that were run and were able to retrieve data that had previously been added to the cache. This value increases whenever a Get object retrieves data or metadata from the cache. This value does not decrease, and is cumulative across multiple sessions. It returns to zero only when the cache itself is closed.

**Put Obj Count**

The current number of Put Objects that loaded data values retrieved from a procedure into the cache. This value increases whenever a Put object adds data or metadata to the cache. This value does not decrease, and is cumulative across multiple sessions. It returns to zero only when the cache itself is closed.

**Remove Obj Count**

The current number of Remove Objects that removed data values from the cache in response to the LRU Prune process. This value increases whenever a Remove object removes data or metadata from the cache. This value does not decrease, and is cumulative across multiple sessions. It returns to zero only when the cache itself is closed.

**LruPrune Entries**

The number of Least Recently Used entries removed from the cache to make room for metadata or data that must be added to the cache in response to a query issued from a new procedure. Least Recently Used entries are the oldest entries in the cache that have not been requested by a Get object for reuse by a procedure. This value increases whenever data entries must be removed from the cache to clear memory space for new data or metadata from a Put object. This value does not decrease, and is cumulative across multiple sessions. It returns to zero only when the cache itself is closed.

**LruPrune Memory**

The amount of memory freed when Least Recently Used entries were removed from the cache to make room for metadata or data source values that must be added in response to a query issued from a new procedure. Least Recently Used entries are the oldest entries in the cache that have not been requested by a Get object for reuse by a procedure. Note that this value is cumulative, that is, it represents the amount of memory freed by each LRU remove operation. It does not represent the current amount of free memory.

**Clear Count**

The number of Clear Cache events initiated by users during the current session. Every time a user clicks the Clear Cache command on the Administration Console menu bar, this value increases. Procedures that include a command to clear the cache also cause this value to increase. This value does not decrease, and is cumulative across multiple sessions. It returns to zero only when the cache itself is closed.

**Understanding Cache Group Entries**

Cache entries can be grouped by User ID or the path to the master file from which the data in the entry was retrieved. Both groupings give you an idea of the origin of data transferred to the cache, and help you assess how recently data in the cache was assigned to it or retrieved from it.

The Group by subsection can appear directly underneath the row for each active cache, as shown in the following image. This subsection opens when user activity causes values to be placed in it during the current session, and remains visible until a User clears the cache or an Application Server shutdown closes the cache.

DataValues	50000	3	54	51	0	3	0	0	0	19
Group by	Scope	Path	User			Count	MemoryK	Oldest Age	Last Ref	
	User					3	54	389s	388s	

This subsection displays additional summary cache statistics grouped by Scope, Path, or User. When grouped by Scope, statistics in this section identify summary statistics for all users and paths within the cache. When grouped by User, statistics in this section identify summary statistics for each individual User who added data or metadata to the cache. The section lists one row of statistics for each User. When grouped by Path, statistics in this section identify summary statistics for each individual resource from which data or metadata was added to the cache. The section lists one row of statistics for each Path.

Using these grouping options, you can identify the IBFS paths that were retrieved by queries in this session, and assess the statistics in this subsection by session, user, or query as represented by an IBFS path.

Each option identifies the following group statistics.

#### **Count**

The number of metadata or data source entries currently held in the cache for each user or path, depending upon the selected Group By option. If the Group By option is set to Global, the value will match that of the whole cache.

#### **MemoryK**

The amount of memory occupied by the metadata or data source entries currently held in the cache for each session, user, or path, depending upon the selected Group By option. If the Group By option is set to Global, this value will match that of the whole cache.

#### **Oldest Age**

The number of minutes that the oldest metadata or data source entry has been held in the cache for each user or path.

#### **Last Ref**

The number of minutes that have elapsed after the most recent call for data from the cache.

Caches begin to display statistics when they are initiated by system operations, and close their display of statistics when they are closed by an Application Server shutdown.

Statistics on the page are not logged or stored. With the exception of statistics in the Group By subsection and the Current Entries and Current Memory statistics, they are cumulative and persist from session to session. Current statistics serve as a snapshot of the current state of the caches. Cumulative statistics serve as an ongoing record of the activity that took place over the life of each cache.

## DBA Password Settings

The DBA password defines access to data sources on the Reporting Server. Each data source description can specify which passwords are acceptable for accessing the data source. Each password may also be associated with specific access types, conditions, and rules that limit access down to the row level, if necessary.

The SET PERMPASS=*password* command establishes a password that the user cannot change for access to data sources. You can assign a value to this command this in the SERVER as SET PERMPASS=&FOCSECUSER. You can control whether a PERMPASS command is sent to the Reporting Server with each request with the DBA Source (IBIF\_DBAPASS\_SRC) setting.

Database security is described in the *Describing Data With TIBCO WebFOCUS Language* manual.

By setting the DBA password for each request, you establish a single sign on from Managed Reporting to the data source on the Reporting Server.

TIBCO ReportCaster also supports the DBA password, which is sent in encrypted form to TIBCO ReportCaster. The DBA password cannot be assigned a TIBCO ReportCaster group ID because a single password can be associated with multiple groups. It can be set to the domain ID, the user HREF, or to a user-specified variable.

### **Procedure:** How to Set the Middle-Tier DBA Password

1. In the Administration Console, on the Configuration tab, under the Application Settings folder, click *Client Settings*.
2. Leave the DBA Source (IBIF\_DBAPASS\_SRC) field at its default setting, OFF, to prevent the client from sending the Managed Reporting Server User ID with each Reporting Server Database request.
3. Click IBIMR\_user in the DBA Source (IBIF\_DBAPASS\_SRC) list to send the Managed Reporting User ID to the Reporting Server with each database request.
4. Click Save.

When you receive a message that the change was saved successfully, click OK,

## Obtaining the Identity of the User

To access the user ID in a report request, use the protected Reporting Server variable &FOCSECUSER. This variable contains the connecting user ID, except when Reporting Server security is OFF. &FOCSECUSER is recommended over previous approaches, such as the GETUSER and CNCTUSR subroutines.



To set a DBA password from the connected user ID that cannot be changed in a procedure or configuration file, you can place the following sample code anywhere in the Reporting Server profile (edasprof.prf):

```
SET PERMPASS = &FOCSECUSER
```

For more information about DBA security, see the *Describing Data With TIBCO WebFOCUS Language* manual.

## Deferred Receipt Processing

Deferred Receipt is a Managed Reporting feature that allows users to submit a Managed Reporting procedure that executes in the background. The user then views the finished report output from the Deferred Report Status interface in Managed Reporting. This is in contrast to procedures submitted for immediate execution, where the browser waits for the request to finish.

From a security perspective, deferred requests are accepted by the Reporting Server in the same way as immediate requests. If Reporting Server security is enabled, the deferred request must connect with a valid Reporting Server user ID and password.

When a request completes, its output is stored in a file on the Reporting Server, in the *drive*: \ibi\svnn\wfs directory, where *nn* is the number of the current release. The output is accompanied by a corresponding file that contains the user ID that submitted the request and other information. The Reporting Server ensures that only the user who submitted the deferred job can retrieve, delete, and check the status of the output file. The Reporting Server Administrator (the user identified by the *server\_admin\_id* keyword in the *edaserve.cfg* file) can also view and delete any deferred output, but can do so only at the file level or by using the Reporting Server Console.

**Note:** When you delete a deferred request, a confirmation message appears, by default. A deletion requires two clicks. You can choose to suppress the confirmation message, meaning a deletion requires only one click. This is done using the setting described in *Deferred Reporting Settings*. Making a large number of deletions is faster when you suppress the confirmation message.

Access to the *dfm\_dir* directory should be restricted so that the user ID that started the Reporting Server has read/write access. Read access should be controlled so that unauthorized users cannot gain access to the directory.

A deferred ticket is stored in the Managed Reporting Repository for each deferred request. The tickets are stored by each Managed Reporting user. Users can only see their own deferred tickets, except for an administrator who has access to Manager Mode. The ticket contains the node of the Reporting Server on which the output resides.

When a user requests Deferred Status, all of the tickets belonging to the user are processed at once. If credentials are required to retrieve status from one of the servers, the dynamic server sign-in form appears. If one or more of the servers is temporarily unavailable, the status of those tickets display as unknown.

If a user has submitted a deferred request one day with the user ID user1, and then submits the same request the next day with the ID user2 and checks deferred status, the user will be unable to access the request from the previous day and will see an error message.

To access the first report, the user needs to close the session and sign in to the Reporting Server as user1.

## Stopping a Report Request

Administrators can stop a running report request by using request parameters in the URL.

### **Reference:** Stopping a Self-Service Request in a Legacy Environment

The following request parameters enable users to stop any report request or group of requests from legacy self-service applications or environments. The parameters are specified in the URL of the request as follows:

```
http://server:port/context/WFServlet?  
IBIWF_action=STOPREQ&IBIWF_USER_REQUEST_ID=ALL
```

Stops all requests initiated from the current browser session.

```
http://server:port/context/WFServlet?  
IBIF_ex=procedure_name&IBIWF_USER_REQUEST_ID=value
```

Runs the report procedure specified by IBIF\_ex and assigns an arbitrary value specified by the IBIWF\_USER\_REQUEST\_ID parameter. The IBIWF\_USER\_REQUEST\_ID parameter value in this instance cannot be ALL, as it is a reserved keyword value to stop all requests.

If a request contains an arbitrary value for the IBIWF\_USER\_REQUEST\_ID parameter, a user could stop a specific request or a group of requests by using the following URL and specifying the IBIWF\_USER\_REQUEST\_ID value of the request or group of requests to stop:

```
http://server:port/context/WFServlet?  
IBIWF_action=STOPREQ&IBIWF_USER_REQUEST_ID=value
```

If the request URL contains multiple procedure names with the same IBIWF\_USER\_REQUEST\_ID value, all report requests are stopped.

Once the request is canceled, the following message is displayed:

```
Reporting server request terminated by operator.
```

If the request is stopped while data is already being output, the following message displays in the report output:

`This report is invalid because the data retrieval has been killed or the job has been stopped.`

If report output is PDF and the request is stopped while data is already being output, the following message displays:

`The File is damaged and could not be repaired.`

**Note:** The *Stop Request* menu option does not stop deferred requests or TIBCO ReportCaster jobs.



## Authentication and Authorization

---

This topic explains how to configure authentication and authorization in the WebFOCUS Client. Authentication is the process of identifying users or programs. Authorization is the process of determining the capabilities and access privileges of authenticated users or programs.

Authentication may be performed by WebFOCUS or by an external source, such as an LDAP directory. Users or programs may also be pre-authenticated, which means that one party trusts that another party has taken responsibility for authentication. Authorization may also be internal or external. The simultaneous use of multiple authentication and authorization sources is supported.

**In this chapter:**

- ☐ [Understanding Authentication](#)
  - ☐ [Configuring Pre-Authentication, External Authentication or External Authorization](#)
  - ☐ [Security Zones](#)
  - ☐ [Anonymous Access](#)
  - ☐ [Internal Authentication](#)
  - ☐ [Pre-Authentication](#)
  - ☐ [External Authentication](#)
  - ☐ [Understanding Authorization](#)
  - ☐ [Understanding Internal Authorization](#)
  - ☐ [Understanding External Authorization](#)
  - ☐ [Special Considerations for Microsoft Office Drill-Down Links](#)
  - ☐ [Special Considerations for TIBCO WebFOCUS Deployments With Separate ReportCaster Installations](#)
-

## Understanding Authentication

Authentication is the process by which a system identifies a user or program. Authentication may involve checking the user ID and password supplied interactively by an individual or presented automatically by a program. These methods are known as form-based authentication. Users or programs may also be pre-authenticated, which means that one party trusts that another party has taken responsibility for authentication.

There are many options for authenticating users. By default, users are authenticated against information stored in the internal repository. Internal authentication that uses WebFOCUS account policies is very secure, but many organizations already maintain user account information in a centralized location outside of the product.

You can configure WebFOCUS to authenticate users to these external sources, such as a Microsoft Active Directory (AD), a Lightweight Directory Access Protocol (LDAP) directory, or information stored in a relational database management system (RDBMS) table. WebFOCUS can also be configured for pre-authentication. In pre-authentication, WebFOCUS trusts the authentication performed by another system, such as a web server, an Internet identity provider, a Web Access Management system, or another application.

Frequently, different requirements for authentication exist at different points within an application. It is important to consider the following early in the planning phase:

☐ Where does authentication occur?

Typically, the decision about where authentication should occur is made based on which platforms have the most robust security enforcement and the most sensitive data. Authentication may take place when signing in to the operating system, and a further layer of authentication might be required when accessing a particular application. By contrast, you may decide that the authentication that takes place when signing in to the operating system is sufficient for all needs. In this case, you would allow all previously authenticated users to access resources without re-authenticating.

☐ How will passwords be managed?

Which passwords will be stored and where in the environment will they be stored? When do passwords expire? What are the complexity rules that apply to passwords, specifying length and allowed characters?

☐ How often will the user need to provide credentials to sign in to your system?

To improve usability, you may want to minimize the number of disruptions in processing and passwords to be remembered.

## Supporting Different Security Models in Different Environments

Companies often implement different security models in development, test, and production environments. For example, in a production environment, the WebFOCUS Reporting Server is typically configured to use a single service account to access data on behalf of authenticated users. This enables reporting system users to request reports generated from data stored in an RDBMS that does not have individual sign-in user IDs for every user. By contrast, in a development environment, developers may have individual RDBMS sign-in user IDs to control individual access to sensitive development data. To support these requirements, you can authenticate users against the WebFOCUS Reporting Server in your development environment and against your usual security provider or single sign-on application in your production environment.

In most cases, the test and production environments share the same security model.

### The Remember Me Feature

When your installation is configured for internal or external authentication, you can enable the *Remember me on this computer* feature to give users the option of bypassing the Sign in page. After successfully authenticating once, a trusted sign-in cookie is stored locally on the workstation, for a default period of 14 days. The user password is not stored in the sign-in cookie.

**Note:** Do not enable this feature with pre-authentication. The Remember Me check box is only displayed when users are signing in, so it is never displayed to pre-authenticated users.

### *Procedure:* How to Enable the Remember Me Feature

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page.

1. Under the Security Zones folder, expand the folder for the Security Zone you want to update, and then click *Authentication*.
2. On the Authentication page, click *Remember-Me Authentication*, and then click *Edit*.
3. Select *The login request is always a remember-me request* check box.

**Note:** Do not change values in *The name of the cookie* field or in *The name of the parameter which should be checked for to see if a remember-me has been requested during the login request* field unless advised to do so by Customer Support.

4. To use a secure cookie for all remember-me logins, select the *Use secure cookie* check box.

**Note:** When you select this check box, the `/secure` flag is set for this cookie, ensuring that it will only be sent over an https connection.

5. Click *OK*.
6. In the Actions section, click *Enable*, and then click *Save*.
7. When you receive a confirmation message, click *OK*.
8. When you receive a message to reload the web application, click *OK*.
9. Sign out of your current session.
10. Stop and restart the server.
11. Sign in again as an administrator, return to the Administration Console, and test the new configuration.

### **Procedure:** How to Disable the Remember Me Feature

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Zones folder, expand the folder for the Security Zone you want to update, and then click *Authentication*.
3. On the Authentication page, click *Remember-Me Authentication*, and then click *Edit*.
4. Clear *The login request is always a remember-me request* check box.
5. Clear the *Use secure cookie* check box, if it is selected.

**Note:** Do not change values in The name of the cookie field or in The name of the parameter which should be checked for to see if a remember-me has been requested during the login request field unless advised to do so by Customer Support.

6. Click *OK*.
7. In the Actions section, click *Disable*, and then click *Save*.
8. When you receive the confirmation message, click *OK*.
9. When you receive the message to reload the web application, click *OK*.
10. Sign out of your current session.
11. Stop and restart the server.
12. Sign in again as an administrator, return to the Administration Console, and test the new configuration.



## Configuring Pre-Authentication, External Authentication or External Authorization

Configuring pre-authentication, external authentication, or external authorization requires you to perform the following tasks:

1. Create a WebFOCUS administrator account whose name matches an account in the external authentication source.
2. It is strongly recommended that you ensure back-up access to WebFOCUS before configuring pre-authentication or external authentication. For external authentication or authorization, this means configuring the superuser. For pre-authentication, this means also enabling the alternate zone.
3. Configure a trusted connection between the WebFOCUS Client and the WebFOCUS Reporting Server.
4. If you wish to use separate authentication methods for default authentication, alternate authentication, mobile authentication, or portlet authentication, configure the security zones to support your requirements.
5. For pre-authentication, configure pre-authentication as appropriate for your needs. For external authentication or authorization, configure a security provider on the WebFOCUS Reporting Server and then configure the WebFOCUS Client to authenticate to the WebFOCUS Reporting Server.
6. For external authorization, map external groups.

### **Procedure:** How to Create a TIBCO WebFOCUS Administrator Account for External Sources

Since the default WebFOCUS administrator account *admin* generally does not exist in the external source, it cannot be authenticated once pre-authentication or external authentication has been successfully configured. The account that you create will exist in both WebFOCUS and the external source so that you can use it for administrative access to WebFOCUS once you have restarted WebFOCUS in its new authentication configuration.

The user ID of the WebFOCUS administrator account that you create must match an account in the external source, although it does not need to be an administrator in the external source. For example, if you are configuring pre-authentication to a Web Access Management system, the WebFOCUS user name should be identical to the Web Access Management user ID.

If you are configuring external authentication to LDAP, the WebFOCUS user name should be identical to the LDAP user name. If you are configuring pre-authentication to Windows, specify the Windows account without the domain name.

1. In the Security Center, under Users, click *New User*.
2. Type an account name that is identical to the user ID of an account in the external source.
3. Type a password and the password confirmation.

**Note:** WebFOCUS ignores this password when you sign in using pre-authentication or external authentication. However, if you have configured pre-authentication in the default zone, enabled the alternate zone, and left External Security Type blank, this password will be verified if it is supplied during sign in from the alternate zone.

4. Optionally, type a description and an email address.
5. Click *GroupAdmins*, in the Create in Group list. Leave the account status as *Active*.
6. Click *OK* to save your changes and exit the New User dialog box.
7. Close or move away from the Security Center.

You have now created the WebFOCUS account that you will use for administrative access once you have restarted WebFOCUS in the new authentication configuration. You can now proceed to enabling superuser access to WebFOCUS.

### **Procedure:** How to Enable Superuser Access

Superuser access overrides all other security rules. The superuser account can be internally authenticated to WebFOCUS, even if pre-authentication, external authentication, or external authorization is misconfigured or unavailable. You should use the superuser account only if you encounter sign-in problems with the administrator account while configuring authentication. After validating that the configuration has been successful, you should either disable superuser access or protect the superuser password.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Configuration folder, click *Advanced*.
3. In the Root User field, type the superuser account name. In the Root Password field, type the superuser password, then click *Save*.

**Note:** Do not specify the WebFOCUS administrator account that you created for use after configuration is complete.

4. When you receive a message stating that the changes were saved successfully, click *OK*.
5. When you receive a message asking you to clear the cache, click *OK*.
6. In the Administration Console menu bar, click *Clear Cache*.
7. When you receive a message confirming that the cache is cleared, click *OK*.

You have now enabled superuser access for the named account. If you are configuring pre-authentication, you can enable the alternate zone so that the superuser can sign in, even if pre-authentication is misconfigured.

If you are configuring external authentication, you can test superuser access by signing out and then signing in with the new superuser credentials.

Once you have verified superuser access, you can proceed by configuring a trusted connection between the WebFOCUS Client and the WebFOCUS Reporting Server.

**Procedure: How to Configure a Reverse Proxy for Apache Tomcat**

If you are planning to use a reverse proxy configuration with an Apache Tomcat™ application server, you must configure a setting in the server.xml file to ensure that all URL calls use the address of the web-facing proxy server, instead of the internal server. Otherwise, some features, such as drill downs in Microsoft® Excel® 2007 reports, retrieve information from the internal host machine instead of the proxy.

To modify the Apache Tomcat server.xml file, perform the following steps:

1. Navigate to the following directory

```
<Tomcat_Home>\conf
```

where:

```
<Tomcat_Home>
```

Is the location on your system where Apache Tomcat is installed.

2. Open the server.xml file with a text editor.
3. Search for the Coyote/JK2 AJP 1.3 connector block.
4. Add the proxyName and proxyPort parameters, as shown in the following example:

```
<!-- Define a Coyote/JK2 AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
    enableLookups="false" redirectPort="8443" debug="0"
    protocol="AJP/1.3" proxyName="WEB-FACING PROXY_SERVER"
    proxyPort="WEB FACING PROXY_PORT" />
```

5. For the proxyName parameter value, specify the fully qualified host name of the web-facing proxy server.
6. For the proxyPort parameter value, specify the port number of the web-facing proxy server.
7. Save the changes to the server.xml file.
8. Restart the Apache Tomcat application server.

## Security Zones

In some WebFOCUS deployments, it may be useful to support multiple authentication methods in a single environment. For example, you may wish to pre-authenticate end users with a Web Access Management system, but allow administrators to sign in with a user ID and password. In another example, you may need to pre-authenticate employees with Windows Authentication, but present customers with a Sign in page where they can type their LDAP user IDs and passwords.

The WebFOCUS mobile and portal options also have special authentication requirements. To support different authentication methods based on configurable criteria, WebFOCUS uses security zones. Each zone is defined by a configuration file located in the `drive:\ibi\WebFOCUS82\config` directory in Windows, or in the `installdirectory/ibi/WebFOCUS82/config` directory in UNIX or Linux.

The following table describes the security zones.

Zone	Configuration File	Description
Default zone	securitysettings.xml	By default, supports form-based authentication for any request not processed by one of the other zones.  <b>Tip:</b> Configure this zone to use the primary type of authentication used by your user base.
Alternate zone	securitysettings-zone.xml	By default, supports form-based authentication for administrators who access WebFOCUS with the web browser installed on the WebFOCUS Client machine.
Portlet zone	securitysettings-portlet.xml	Defines the authentication method for WebFOCUS Open Portal Services products, including SharePoint.

The default zone is always enabled. Configure the primary authentication method here.

Within the default zone you can configure one pre-authentication method in addition to form-based authentication. The ability to configure two methods of authentication in this zone allows you to maintain pre-authentication credentials for users of that zone but require them to specify sign-in credentials using the default Sign in page or a customized Sign in page whenever it is necessary to override their pre-authentication credentials.

For example, if you assign Integrated Windows Authentication (IWA) to the default zone in addition to form-based authentication, you can rely on IWA pre-authentication when users sign in from their own workstation, and impose form-based authentication on them when they sign in from any other workstation.

Users who sign in from a workstation other than their own will be required to present their credentials for each sign-in attempt, overriding the default IWA credentials established for that workstation and helping to ensure that unauthorized individuals using that workstation cannot gain access based on those default credentials. Users who sign in from their own workstation can avoid the requirement to present their User ID and Password at each sign-in attempt, relying on Integrated Windows Authentication instead.

However, if you configure two alternative authentication methods for the default zone, and define a custom sign-out page for the pre-authentication method, that page will override the default sign-out page. When adopting this configuration, be aware that only a single custom sign-out page can be configured.

The alternate zone allows you to set up secondary authentication methods to be used based on user network location. By default, the alternate zone is not enabled. If enabled, it is preconfigured to process requests coming from the network address localhost, or 127.0.0.1 and ::1 (TCP/IPv4 and TCP/IPv6, respectively), which you can change. You can add or remove addresses, such as an administrator workstation address, a reverse proxy, or another machine that is more convenient for Remote Desktop connections.

Addresses in the configuraton support wildcards, allowing you to specify a range of IP addresses, in addition to individual addresses. The asterisk (\*) matches any number of characters, and the question mark (?) matches a single character, as shown in the following excerpt from a sample securitysettings-zone.xml file.

```
<property name="filterChainEnabled" value="true"/>
<property name="filterChainPatternEnabled" value="true"/>
  <property name="filterChainPatterns">
    <list>
      <value>/**</value>
    </list>
  </property>
<property name="filterChainIPAdresseEnabled" value="true"/>
<property name="filterChainIPAddresses">
  <list>
    <value>127.0.0.1</value>
    <value>172.30.240.1</value>
    <value>172.30.???.??1</value>
    <value>172.30.239.*</value>
  </list>
</property>
```

**Note:** The audit log file records the TCP/IP address associated with each user session. This information can be useful in troubleshooting configuration issues with a security zone.

When the Sign in page is presented to users in the alternate zone, they are redirected to the WebFOCUS Sign in page. The zone indicator is appended to the sign-in URL, for example:

[http://localhost/ibi\\_apps/zone/signin](http://localhost/ibi_apps/zone/signin)

The mobile and portlet zones are preconfigured to support these optional products and do not generally need to be changed.

## Specifying a Sign-out URL by Zone

You can specify a different sign-out URL for each zone. If you do not specify the sign-out URL for a zone, the URL defaults to \signout, which is the default value in the Custom logout target URL setting. However, this setting is not activated for an individual zone unless you select the Enable custom logout target URL check box.

Partially-qualified URLs are incomplete URLs that imply a location under the ibi\_apps folder. You can assign such a URL to this setting only if public access is enabled. If public access is disabled, partially-qualified URLs will not perform as expected and you must use fully-qualified URLs that do not imply a location under the ibi\_apps folder in this setting.

In a single sign on (SSO) environment, signing out of WebFOCUS does not necessarily sign the user out from the authenticated SSO product session, since authentication credentials remain with the third-party authentication provider. In this case, you may wish to specify the sign-out redirect URL to a URL that ends the SSO product session, if one exists. For example, the sign-out URL for WebSEAL may be:

<http://webseal.domain.com/pkmslogout>

The sign-out URL for Siteminder may be:

<http://siteminder.domain.com/logout.html>

## Anonymous Access

Anonymous access, also known as public access, is useful for applications that require neither authentication nor personalization. It allows unauthenticated users to list and run resources located in the WFC/Repository/Public folder, but makes no other privileges, such as the ability to create or edit resources, available to them. The limitations built into this mode of access enable administrators to protect the integrity of resources designed for general use, even while making them available to all users.

Anonymous access is disabled, by default. In order to make Anonymous access available, the Anonymous Authentication method must be enabled in the Security Zones that will require anonymous access

When you enable Anonymous Authentication in a security zone, the WebFOCUS Client supports anonymous or unauthenticated access to resources in the WFC/Repository/Public folder, as well as to procedures on the WebFOCUS Reporting Server. If you would like anonymous users to have access to other content stored in the repository, you can create rules that grant anonymous users access to those additional resources, as described in the topic, [Changing the Security Policy for Anonymous Users](#) on page 230. The WebFOCUS Reporting Server credentials used by the Anonymous User (IBI\_ANONYMOUS\_USER) setting are Reporting Server Anonymous User ID (IBI\_WFRS\_ANONYMOUS\_USER) and Reporting Server Anonymous Password (IBI\_WFRS\_ANONYMOUS\_PASS). All of these settings appear on the Advanced page of the Security tab.

A separate session is created for each anonymous user. These sessions are associated with each user by a non-persistent WF-JSESSIONID cookie stored in the web browser. Information that is unique to each anonymous user, such as foccache tokens and global amper variables is also tracked. All anonymous sessions have the same effective policy, that of the user account specified by the Anonymous User (IBI\_ANONYMOUS\_USER) setting.

Anonymous Authentication should be disabled when WebFOCUS is configured for pre-authentication, because this configuration limits access to specific pre-authenticated users. WebFOCUS supports public access when configured for external authentication, but additional considerations apply.

For more information about configuring public access for external authentication, see [External Authentication](#) on page 321.

You can specify the default user ID for unauthenticated access with the Anonymous User ID (IBI\_ANONYMOUS\_USER) setting on the Advanced page of the Security tab. By default, this user ID is named public.

### ***Procedure:* How to Enable Anonymous Access for Individual Security Zones**

Anonymous Access is disabled, by default. To enable it for the Default Security Zone or the Alternate Security Zone, you must enable the Anonymous Authentication method.

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Zones folder, expand the folder for the Security Zone you want to update, and then click *Authentication*.
3. Click the *Anonymous Authentication* entry. In the Actions section, click *Enable*, and then click *Save*.

or

Right-click the *Anonymous Authentication* entry, and click *Enable*. In the Actions section, click *Save*.

4. When you receive the confirmation message, click *OK*.
5. When you receive the message to reload the web application, click *OK*.
6. Sign out of your current session.
7. Stop and restart the application server.
8. Sign in again as an administrator, and test the new configuration.

### ***Procedure:* How to Disable Anonymous Access for Individual Security Zones**

Once Anonymous Access is enabled for an individual Security Zone, you can disable it for that zone by disabling the Anonymous Authentication Method.



We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Zones folder, expand the folder for the Security Zone you wish to update, and then click *Authentication*.
3. Click the *Anonymous Authentication* entry. In the Actions section, click *Disable*, and then click *Save*.

or

Right-click the *Anonymous Authentication* entry, and click *Disable*. In the Actions section, click *Save*.

4. When you receive the confirmation message, click *OK*.
5. When you receive the message to reload the web application, click *OK*.
6. Sign out of your current session.
7. Stop and restart the application server.
8. Sign in again as an administrator, and test the new configuration.

#### ***Procedure:* How to Disable Anonymous Access for All Security Zones**

To disable Anonymous Access throughout the application, remove the name and password assigned to the Anonymous user settings in the Advanced Security settings page, and then delete the Public User in the Security Center.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Configuration folder, click *Advanced*.
3. Clear the values assigned to the Reporting Server Anonymous User ID field and Reporting Server Anonymous User Password field.
4. In the Security Configuration section, click *Save*.
5. When you receive the changes have been successfully saved message, click *OK*.
6. When you receive the Please clear cache in order for these change to take effect message, click *OK*.
7. In the Administration Console menu bar, click *Clear Cache*.
8. When you receive the confirmation that the cache is cleared, click *OK*.
9. Navigate to the Security Center.
10. In the Users pane, under the Users folder, click the *Public* entry, and then click *Delete User*.

When you receive a confirmation message, click Yes to delete the user.

11. Click *Close*.

### **Procedure:** How to Specify a Different Account for the Anonymous User

To specify a different user account for the Anonymous User, create a new user account and then change the name assigned to the Anonymous User ID (IBI\_Anonymous\_User) setting to the name assigned to the new user account.

1. In the Security Center, on the Users & Groups tab, click *New User*.
2. In the New User dialog box, type a user name for the new anonymous user account, and optionally, add a description.

**Note:** Do not specify an email address or password for the account.

3. Click *Anonymous* in the Create in Group list, and then click *Active* in the Status list.
4. Click *OK*.

You have now created the account for the new anonymous user.

5. Open the Administration console, and click the *Security* tab.
6. In order to designate the new user as the default Anonymous User ID, perform the following steps:
  - a. Under the Security Configuration folder, click *Advanced*.
  - b. In the Anonymous User ID (IBI\_ANONYMOUS\_USER) field, type the name of the user Account you just created in the Security Center.

You have now configured WebFOCUS to use the new user account as the anonymous user.

### **Reference:** Changing the Security Policy for Anonymous Users

By default, anonymous users have access to resources in the Public folder. If you would like anonymous users to have access to other folders or to portals, you can create new rules to enable access. We recommend that you manage the security policy for anonymous users by placing rules on the Anonymous group and placing the user account specified by the User field in the Anonymous Authentication settings for a Security Zone in that group, rather than directly placing rules on the user account

For more information about creating rules, see [How to Create a Rule on a Group, User, or Role](#) on page 471.

## Making BI Portals Available to Anonymous Users

In the WebFOCUS Enterprise Edition, administrators can make BI Portals intended for general use available to anonymous users working in security zones that have enabled Anonymous Access.

Basic portals are located on the Portals Node and in the Portals area of the Hub. They are not located in workspace folders or in the Public folder. To make them available to anonymous users, an administrator must:

- ❑ start pageCreate a rule that makes the BIPViewOnly role available to the EVERYONE group and apply it to the basic portal.
- ❑ If a basic portal contains reports, charts, or other content resources, an administrator must also create a rule that makes the ListAndRun role available to the EVERYONE group and apply it to that basic portal.

Collaborative portals and designer portals are located in workspace folders or in the Public folder. Therefore, administrators must assign rules to the Public folder or to those workspace folders that contain these portals and their content resources to make the collaborative and designer portals they contain available to anonymous users.

A rule making the ListAndRun role available to the EVERYONE group is assigned to the Public folder, by default. Therefore, to make collaborative and designer portals that are located in the Public folder available to anonymous users, an administrator must:

- ❑ Create a rule that makes the BIPViewOnly role available to the EVERYONE group on the Public folder by selecting the folder and children option.
- ❑ If the collaborative portal or designer portal contains content resources located in other workspaces, an administrator must also create rules that make the BIPViewOnly and ListAndRun roles available to the EVERYONE group on those workspaces.

To make collaborative and designer portals that are located in workspaces outside of the Public folder available to anonymous users, an administrator must:

- ❑ Create a rule that makes the BIPViewOnly and ListAndRun rules available to the EVERYONE group on the workspace folder that contains the portal, and on any charts, reports, or other content resources contained in that portal.
- ❑ If the collaborative portal contains resources located in other workspaces, an administrator must create rules that make the BIPViewOnly and ListAndRun roles available to the EVERYONE group on those workspaces, or grant General Access to the workspace that contains the portal.

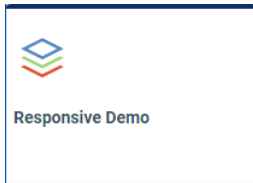
Note that this second method assigns all users to the Basic User group when accessing the workspace that contains the portal, limiting all users to list and run privileges for the content resources in that portal.

For more information about how to assign a rule, see [How to Create a Rule on a Group, User, or Role](#) on page 471 or [How to Create a Rule on a Content Resource](#) on page 470.

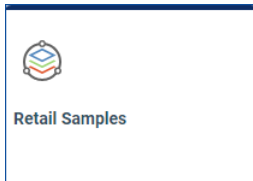
Limitations in the AnonymousRestrictions role, which is assigned to the Anonymous users group, by default, prevent individuals working under the Anonymous User ID from affecting the content or performance of BI Portals made accessible to them.

## Distinguishing Basic Portals from Collaborative Portals and Designer Portals

When working in the tile view, portal icons appear in the content section. Icons for basic portals contain a stack of squares, as shown in the following image.



Icons for collaborative and designer portals contain a stack of squares surrounded by a circle, as shown in the following image.



There are no other distinguishing characteristics between entries for basic portals and other portal types in the tile view.

A more reliable test is the presence or absence of the Properties option on the menu that opens when you right-click a portal icon:

- ☐ Basic portals do not include the Properties option in their shortcut menu.
- ☐ Collaborative and designer portals do include the Properties option in their shortcut menu.

## Form Based Authentication

Form based authentication is the default method of authentication for each of the security zones. To authenticate a user request in this method, the WebFOCUS Client presents the familiar Sign in page to a user, and uses an HTML Form tag to convey the User ID and Password collected during the sign-in process to the WebFOCUS Reporting Server for validation.

### **Procedure:** How to Customize Form-Based Authentication Settings

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Zones folder, expand the folder for the Security Zone you wish to update, and then click *Authentication*.
3. Click the *Form Based Authentication* entry.
4. In the Actions section, click *Edit* to open the Edit Form Based Authentication Settings dialog box.

In that dialog box, all three check boxes are cleared, by default.

5. Click *OK* to accept the default settings.
6. In the Actions section, click *Save*.
7. When the confirmation message opens, click *OK*.
8. When you receive a message to reload the web application, click *OK*.
9. Sign out of your current session.
10. Stop and restart the Application Server.
11. Sign in again as an administrator, and test the new configuration.

## Internal Authentication

By default, users are authenticated against information stored in the Repository. When users sign in, a salted hash of the user password is generated and compared to the password hash stored for the user in the repository. The user password itself is not stored, and the password cannot be determined from the value of the stored hash.

Passwords are not required for user accounts, by default, but this, like other aspects of the internal authentication process, is customizable. You can specify a custom Sign in page and style it to meet your requirements. You can also configure password and account policies. These policies include whether a password is required, how long a password must be, whether users can change their own passwords, and whether user sign-in information will be remembered.

## Pre-Authentication

In pre-authentication, it is assumed that trusted authentication has already taken place, and user identity information is delivered by one of the methods described in the following topics. In this configuration, no Sign in page is displayed to users. Certain features, such as anonymous access and the ability for users to change their own passwords, should be disabled.

Pre-authentication offers several benefits, such as a single sign on (SSO) experience for users and centralized authentication for administrators, eliminating the need to synchronize passwords between WebFOCUS and another source. Depending on the chosen method of pre-authentication, additional steps may be necessary to ensure that the pre-authentication configuration cannot be compromised. For example, if the pre-authenticated user ID will be passed in an HTTP header, then steps must be taken to ensure that the value of this header cannot be compromised.

## Configuring Pre-Authentication With Central Authentication Service (CAS)

Central Authentication Service (CAS) pre-authentication allows clients such as web applications to authenticate users without gaining access to user security credentials. Instead, the WebFOCUS Client authenticates itself to the CAS server, which then returns a security ticket to the WebFOCUS Client to validate that the connection is secure. The WebFOCUS Client validates the ticket by providing the ticket and its own service identifier to the CAS server, and CAS returns trusted information about whether an individual user has been authenticated.

If the CAS server uses a self-signed certificate, in most cases, you will need to add the certificate authority signing certificate to the trusted root certificates for the JVM used by WebFOCUS.

### ***Procedure:*** How to Configure Pre-Authentication With Central Authentication Service

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Zones folder, expand the folder for the Security Zone you wish to update, and then click *Authentication*.
3. Click the *CAS Authentication* entry.
4. In the Actions section, click *Edit*.
5. In the Edit CAS Authentication Settings dialog box, type the URL for the CAS Login Server, using the format:

<https://CASSERVER.domain.com:port/cas/login>

where:

[CASSERVER.domain.com](#)

Is the network name or IP Address of the server hosting CAS operations.

[port](#)

Is the port to which the CAS Server is connected.

6. Type the URL for the CAS Service Ticket Validator, using the format:

<https://CASSERVER.domain.com:port/cas>

where:

[CASSERVER.domain.com](#)

Is the network name or IP Address of the server hosting CAS operations.

[port](#)

Is the port to which the CAS Server is connected.

7. Type the URL for the CAS Service, using the format:

[https://WebFOCUSSEVER.domain.com:port/ibi\\_apps](https://WebFOCUSSEVER.domain.com:port/ibi_apps)

where:

[WebFOCUSSEVER.domain.com](#)

Is the network name or IP Address of the server hosting WebFOCUS operations.

[port](#)

Is the port to which the WebFOCUS Reporting Server is connected.

8. Click *OK*.
9. Right-click the CAS Authentication entry, and click *Enable*.
10. In the Actions section, click *Save*.
11. When you receive the confirmation message, click *OK*.
12. When you receive the message to reload the web application, click *OK*.
13. Sign out of your current session.
14. Stop and restart the WebFOCUS Reporting Server.
15. Sign in again as an administrator, and test the connection.

**Procedure:** How to Add Your CAS CA Certificate to Your TIBCO WebFOCUS cacerts File

If you are using a self-signed certificate for your CAS Server, you will also need to add the CA certificate of this server to the trusted root certificates for the JVM used by WebFOCUS.

**Note:** This task is not necessary if you are using a certificate signed by a trusted certificate authority.

1. Export your CA Certificate from your CAS site, and save it in the WebFOCUS environment.
2. Shut down the Tomcat server.
3. Navigate to the Tomcat JDK and locate the cacerts file.

Typically, the cacerts file is located in the *drive:\ibi\JDK\jre\lib\security* folder in Windows or the *installdirectory/ibi/JDK/jre/lib/security* folder in UNIX or Linux.

- a. In the folder that contains the cacerts file, open the Command Prompt window, and run the following command:

```
..\..\..\bin\keytool -import  
-alias youralias -keystore cacerts -file path\to\yourca.cert
```

where:

*youralias*

Is the alias assigned to your certificate.

*yourca.cert*

Is the certificate file.

- b. If prompted for a password, type *changeit*. If prompted to import a certificate, type *yes*.
4. Restart the Tomcat server.



**Example: CAS Validation Errors**

CAS validation errors may occur if you are using a self-signed certificate that has not been added to the trusted certificate store. In such cases, you will receive an error similar to the following:

```
[YYYY-MM-DD hh:mm:ss,sss] ERROR
org.jasig.cas.client.validation.Cas20ServiceTicketValidator
http-apr-8080-exec-2 - javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target
javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target
at com.sun.net.ssl.internal.ssl.Alerts.getSSLException(Unknown Source)
.
.
... 60 more
Caused by: sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target
at sun.security.provider.certpath.SunCertPathBuilder.engineBuild(Unknown
Source)
at java.security.cert.CertPathBuilder.build(Unknown Source)
... 66 more
```

**Configuring Pre-Authentication with HTTP BASIC Authentication**

HTTP Basic Authentication delivers an HTTP message containing a user name and password from a client to a server. The server compares the two values from the message to those User IDs and Passwords stored in a database of users who are valid for a designated realm, which is a set of web pages that require authenticated credentials. Based on the results of this operation, the server returns a message stating the status of the authentication.

Because HTTP BASIC Authentication uses the easily reversible Base64 encoding for its messages instead of encryption, it is non-secure unless used with SSL. To configure HTTP Basic Authentication, you must identify the name of the realm affected by the HTTP Basic Authentication, typically, WebFOCUS. This setting directs the authentication request to that section of the database that lists those users who are entitled to view and work with pages within that realm.

**Note:** HTTP Digest authentication is not available in release 8.2.01.

### ***Procedure:* How to Configure HTTP BASIC Authentication**

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Zones folder, expand the folder for the Security Zone you wish to update, and then click *Authentication*.
3. Right-click the *HTTP Basic Authentication* entry, and then click *Edit*.
4. In the Realm name field, accept the default value, WebFOCUS, or type a different name.
5. Click *OK*.
6. Right-click the HTTP Basic Authentication entry, and click *Enable*.
7. In the Actions section, click *Save*.
8. When you receive the confirmation message, click *OK*.
9. When you receive the message to reload the web application, click *OK*.
10. Sign out of your current session.
11. Stop and restart the WebFOCUS Reporting Server.
12. Sign in as an administrator, and test the new configuration.

### **Configuring Pre-Authentication With Java Container Security**

Java containers, such as Apache Tomcat, IBM WebSphere, and Oracle WebLogic, can authenticate users on behalf of WebFOCUS. The Java container uses the `getRemoteUser()` call to provide user IDs to WebFOCUS.

### ***Procedure:* How to Configure JEE Container Based Authentication**

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

You must also build a Java container to support user authentication. For more information, consult the documentation provided by the vendor that supplied your installation of Java.

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Zones folder, expand the folder for the Security Zone you wish to update, typically the Default Security Zone, and then click *Authentication*.
3. In the Actions section of the Authentication Page, click *Options*.
4. In the Authentication Options dialog box, select the *Enable custom logout target URL* check box.
5. Accept the default value `/signout`, or type a custom logout target URL in the Custom logout target URL field, and click *OK*.
6. On the Authentication page, right-click *JEE Container Based Authentication*, and then click *Enable*.

All other authentication methods are disabled automatically.

7. To include form-based authentication in the updated Security Zone configuration, right-click *Form Based Authentication*, and then click *Enable*.

To exclude form-based authentication from this security zone, leave Form Based Authentication disabled.

8. Consult your Java container documentation for additional instructions on enabling J2EE authentication.
9. On the Authentication page, in the Security Zones section, click *Save*.
10. When you receive a message that the web security configuration data was saved successfully, click *OK*.
11. When you receive a message advising you to reload the web application in order for these changes to take effect, click *OK*.
12. Sign out of your current session.
13. Stop and restart the WebFOCUS Reporting Server.
14. Sign in again as an administrator and test the new configuration.

## Configuring Pre-Authentication With OpenID Connect

Identity providers, such as Google or Keycloak, deliver authentication services that conform to the specifications of the OpenID Connect protocol.

When Open ID Connect pre-authentication has been enabled, users navigating to the \ibi\_apps context are presented with the sign-in screen of their identity provider instead of the WebFOCUS sign-in screen. Users type their credentials on that screen and send them to the OpenID Connect identity provider. When the identity provider determines that the credentials presented by WebFOCUS and the end user are authenticated, the user is redirected to WebFOCUS.

WebFOCUS prepares a client authentication message that returns its own Client ID to the identity provider and can also include scope identifiers that request additional information about the end user.

When the identity provider authenticates the credentials presented by WebFOCUS, it returns the requested user information, and the authenticated user can begin a session.

When users end their session, they must be directed to the sign-out page used by the identity provider instead of the standard WebFOCUS sign-out page. From the identity provider sign-out page they can choose to sign in to their OpenID Connect identity provider again or move on to other web sites or applications.

### **Configuring OpenID Connect Authentication Settings at an Identity Provider**

As an application that accepts OpenID Connect user authentication, your installation of WebFOCUS functions as a client or relying party in the OpenID Connect Authentication process, and an administrator must create an account for this party with an OpenID Connect identity provider.

Even though each OpenID Connect identity provider maintains slightly different configurations and requirements, all providers must conform to the OpenID Connect standard.

Administrators must expect to provide a Client Name and additional information that uniquely identifies their installation of WebFOCUS to the identity provider. This additional information can include the Root URL for their installation of WebFOCUS, and one or more Valid Redirect URIs that identify the location of the resources that process responses delivered from the identity provider during the sign-in process.

The identity provider creates and provides administrators with a Client ID and a Client Secret that is unique to each installation of WebFOCUS. The identity provider also identifies its Custom Logout Target URL. When users end their WebFOCUS session, they are directed to this URL, where they are free to sign in again to the identity provider or move on to other tasks. Administrators include all of these values in their configuration of the Open ID Connect configuration.

## Configuring OpenID Connect Authentication Settings Within TIBCO WebFOCUS

The Edit OpenID Connect Authentication Settings dialog box contains the credentials and endpoint URIs that must be delivered to the OpenID Connect identity provider within client authentication messages, as shown in the following image.

The screenshot shows a dialog box titled "Edit OpenID Connect Authentication Settings". It contains the following fields and values:

- Client ID: (empty text box)
- Client Secret: (empty text box)
- User Authorization URI: <https://accounts.google.com/o/oauth2/auth>
- Access Token URI: <https://www.googleapis.com/oauth2/v3/token>
- User Info URI: <https://www.googleapis.com/oauth2/v2/userinfo>
- Logout URI: <https://www.google.com/accounts/Logout>
- Attribute Name for User ID: name
- ☐ Strip the domain name from User ID
- Optional Scope Values: email
- Resource URI: (empty text box)
- ☐ Retrieve User Groups from the Claims
- Attribute Name for User Groups: (empty text box)
- Client Authentication Method: HTTP POST (dropdown menu)

At the bottom right, there are "OK" and "Cancel" buttons.

In order to communicate with an OpenID Connect identity provider, credentials that identify WebFOCUS as a valid relying party, which is a web site or application that needs to authenticate the identity of an end user, must be established with the identity provider. These values must be included in responses from that relying party to requests to grant access to authenticated users.

- ☐ **Client ID.** Is the unique ID of your installation of WebFOCUS that identifies it to the OpenID Connect identity provider. This value must be unique for every application supported by the identity provider.
- ☐ **Client Secret.** Is a value shared between WebFOCUS and the identity provider that enables both parties to authenticate messages from each other. It must be delivered with each request to the OpenID Connect identity provider. The value assigned to the client secret must be sufficiently random as to be unguessable. For example:

[sGBAyfVL7YWtP6gudLiJbRZV\\_N0dW4f3xEtiIxqtokEAZ6FAsBtgyIq0MpU1uQ7J08xOTO2zwP0OuO3pMVAUTid](#)

Identity providers may require a separate sign in before allowing administrators to review and extract this value.

In order to ensure that OpenID authentication requests are directed to the appropriate endpoints, the following URI information must also be included in the Open ID Connect Authentication Settings dialog box.

- ☐ **User Authorization URI.** Identifies the HTTP endpoint at the identity provider authorization server that can authenticate the end user. Requests for user authentication must be directed to this endpoint.
- ☐ **Access Token URI.** Identifies the HTTP endpoint at the identity provider authorization server that can issue access tokens. Requests for tokens for authenticated users must be directed to this endpoint.
- ☐ **User Info URI.** Identifies the protected resource at the identity provider that maintains user information and can return authorized information about the current user when presented with an access token by the client.
- ☐ **Logout URI.** Identifies the HTTP endpoint at the identity provider to which users must be directed when they choose to sign out of all of their sessions authenticated by the OpenID identity provider. Typically, this is the Sign in page for the OpenID identity provider. At this page, users can sign in again to open another OpenID Connect identity provider session or remain signed out. Note that because the logout redirect URI is defined in this field, there is no need to define a logout URL in the Custom logout target URL field of the Authentication Options dialog box.
- ☐ **Attribute Name for User Id.** Identifies the specific attribute that maps to the WebFOCUS User ID. The default value in this field is *name*. You will most likely replace it with *email*, which indicates that email addresses using the format, *local\_part@domain\_name*, serve as user IDs. Other attribute name values can be used in this field. For more information about the value to use, consult your identity provider. Values assigned to this attribute must be unique.
- ☐ **Strip the Domain Name from User ID.** When this check box is selected, the domain name prefix is automatically cleared from a user ID submitted to the identity provider during the sign-in process. This check box is relevant only to customers who use the *domain name\user ID* format for their user names and work with an OpenID Connect identity provider that does not accept user IDs with a domain name prefix.

- ❑ **Optional Scope Values.** Identifies the names of the optional scope identifiers that can be sent to the identity provider in addition to the required scope identifier, openid. Scope identifiers are requests for specific types of information about the end user who is requesting access to the client. Valid scope identifier values include those defined by the Open ID Connect standard such as, email, address, phone, or profile. The email scope identifier appears in this field, by default, but you can delete it if you and your identity provider do not use it.
- ❑ **Client Authentication Method.** Identifies the HTTP request method that the client authentication message uses to contact the server at the identity provider. The HTTP POST request method is selected, by default. When using this method, client credentials are included in the body of the message. You can also select the HTTP Basic Authentication Scheme request method, in which client credentials are included in the HTTP Authorization Header. We do not recommend that you select the option None, unless your identity provider has advised you to use a different request method not defined in this list.

### Configuring OpenID Connect Pre-Authentication with Google

The Edit OpenID Connect Authentication Settings dialog box is configured with the information required to support pre-authenticated user sign-in requests from Google, by default. Administrators need only add the Client ID and Client Secret, which are provided by Google, and the Attribute Name.

For more information about the Google OpenID Connect API, see <https://developers.google.com/identity/protocols/OpenIDConnect>

#### **Procedure:** How to Configure OpenID Connect Authentication Settings for Google

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Zones folder, expand the *Default Security Zone* folder and then click *Authentication*.
3. Double-click the *OpenID Connect Authentication* entry to open the Edit OpenID Connect Authentication Settings dialog box.
4. Type the name that identifies WebFOCUS as a valid client of the OpenID Connect provider in the Client ID field.

For example:

[292085223830.apps.googleusercontent.com](https://292085223830.apps.googleusercontent.com)

5. Type or copy and paste the Client Secret value provided by Google.

For example:

[GBAyfVL7YWtP6gudLIjbrZV\\_N0dW4f3xEtiIxqtokEAZ6FAsBtgyIq0MpU1uQ7J08xOTO2zwP00uO3pMVAUtiD](#)

6. To establish Google as your OpenID provider, accept the default values in the following fields:

☐ **User Authorization URI.** <https://accounts.google.com/o/oauth2/auth>

☐ **Access Token URI.** <https://www.googleapis.com/oauth2/v3/token>

☐ **User Info URI.** <https://www.googleapis.com/oauth2/v2/userinfo>

☐ **Logout URI.** <https://www.google.com/accounts/Logout>

7. Type a valid attribute name in the Attribute Name for User ID field.

**Note:** You will most likely replace the default value, *name*, with the value, *email*. However, other attribute names can be used in this field. For more information about the value to use, consult your identity provider.

8. If you must ensure that any user ID submitted to the identity provider excludes a domain name prefix, select the *Strip the Domain Name from User ID* check box. Otherwise, leave this check box clear.

**Note:** This check box is relevant only to customers who use the *domain name\user ID* format for their user names and work with an OpenID Connect identity provider that does not accept user IDs with a domain name prefix.

9. Accept the default value, *email*, displayed in the Optional Scope Values field.
10. Accept the default selection, *HTTP POST*, displayed in the Client Authentication Method list.
11. When your configuration is complete, click *OK*.
12. Enable the new configuration as described in [How to Enable OpenID Connect Authentication in a Security Zone](#) on page 249.
13. Save the new configuration as described in [How to Save an OpenID Connect Configuration](#) on page 250.



## Configuring OpenID Connect Pre-Authentication with Keycloak

Keycloak is an open source Identity and access management solution that works with WebFOCUS to provide single-sign-on pre-authentication using the OpenID Connect standard. For more information about Keycloak and its features, see <https://www.keycloak.org/about.html>

For more information and instructions about how to configure an installation of WebFOCUS as a Keycloak client for OpenID Authentication, see the Keycloak Getting Started Guide, located at [https://www.keycloak.org/docs/latest/getting\\_started/index.html](https://www.keycloak.org/docs/latest/getting_started/index.html)

### **Procedure:** How to Configure OpenID Connect Authentication Settings for Keycloak

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Zones folder, expand the *Default Security Zone* folder, and then click *Authentication*.
3. Double-click the *OpenID Connect Authentication* entry to open the Edit OpenID Connect Authentication Settings dialog box.
4. Type the Client ID for WebFOCUS that is identified in the Client ID field of the Settings tab of the Client page for WebFOCUS in Keycloak.

For example: WebFOCUS-HEAD.

5. Type or copy and paste the Client Secret value provided by Keycloak. Typically this is a hexadecimal representation of a randomly-generated value.

For example:

`43b89579-ea9c-4101-b321-56b9dc6ae0f8`

6. In the User Authorization URI field, type:

`http://host:port/auth/realms/realm-name/protocol/openid-connect/auth`

where:

*host*

Is the name or IP address of the host used by Keycloak.

*port*

Is the number of the port on which the Keycloak identity provider listens.

This value is optional, and it should be excluded if the URL uses the default port for the protocol it uses in the scheme, which is port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

*realm-name*

Is the name of the realm you identified for WebFOCUS in Keycloak. For example, WebFOCUSRealm.

For example:

```
http://server01.ibi.com:8080/auth/realms/WebFOCUSRealm/protocol/openid-connect/auth
```

7. In the Access Token URI field, type:

```
http://host:port/auth/realms/realm-name/protocol/openid-connect/token
```

Where *host*, *port*, and *realm-name* identify the host used by Keycloak as described in step 6.

For example:

```
http://server01.ibi.com:8080/auth/realms/WebFOCUSRealm/protocol/openid-connect/token
```

8. In the User Info URI field, type:

```
http://host:port/auth/realms/realm-name/protocol/openid-connect/userinfo
```

Where *host*, *port*, and *realm-name* identify the host used by Keycloak as described in step 6.

For example:

```
http://server01.ibi.com:8080/auth/realms/WebFOCUSRealm/protocol/openid-connect/userinfo
```

9. In the Logout URI field, type:

```
http://host:port/auth/realms/realm-name/protocol/openid-connect/logout?redirect_uri=https://wfhost.ibi.com/context/service/wf_security_logout.jsp
```

Where *host*, *port*, and *realm-name* identify the host used by Keycloak as described in step 6, *wfhost* identifies the name or IP address of the host used by WebFOCUS, and *context* identifies the context used for your installation of WebFOCUS, typically, \ibi\_apps.

For example:

```
http://server01.ibi.com:8080/auth/realms/WebFOCUSRealm/protocol/openid-
connect/logout?redirect_uri=https://wfserver01.ibi.com/ibi_apps/
service/ wf_security_logout.jsp
```

10. Type a valid attribute name in the Attribute Name for User ID field.

**Note:** You will most likely replace the default value, name, with the value, email. However, other attribute names can be used in this field. For more information about the value to use, consult your identity provider.

11. If you must ensure that any user ID submitted to the identity provider excludes a domain name prefix, select the *Strip the Domain Name from User ID* check box. Otherwise, leave this check box clear.

**Note:** This check box is relevant only to customers who use the *domain name\user ID* format for their user names and work with an OpenID Connect identity provider that does not accept user IDs with a domain name prefix.

12. Accept the default value, *email*, displayed in the Optional Scope Values field.
13. Accept the default selection, *HTTP POST*, displayed in the Client Authentication Method list.
14. When your configuration is complete, click *OK*.
15. Enable the new configuration as described in [How to Enable OpenID Connect Authentication in a Security Zone](#) on page 249.
16. Save the new configuration as described in [How to Save an OpenID Connect Configuration](#) on page 250.

## Configuring Pre-Authentication With Other OpenID Connect Identity Providers

Other third-party OpenID Connect providers can pre-authenticate users for WebFOCUS. Even though the information that must be configured in WebFOCUS and at the identity provider must conform to the OpenID Connect standard, the specific configuration requirements for individual identity providers can vary. For more information, see documentation from your OpenID identity provider.

### **Procedure:** How to Configure OpenID Connect Authentication Settings for Other OpenID Connect Identity Providers

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Zones folder, expand the *Default Security Zone* folder, and then click *Authentication*.
3. Double-click the *OpenID Connect Authentication* entry to open the Edit OpenID Connect Authentication Settings dialog box.
4. If your OpenID Connect identity provider assigned you a Client ID, copy and paste that value in the Client ID field.

Or

If you assigned a Client ID to your configuration within the OpenID Connect identity provider, type or copy and paste the value in the Client ID field.

5. Copy and paste the Client Secret value provided by the identity provider in the Client Secret field.
6. Type or copy and paste the following URLs in the fields listed below. All of these values must be provided to you by the identity provider.
  - ☐ **User Authorization URI.** The URL for the http endpoint where the identity provider conducts end user authentication.
  - ☐ **Access Token URI.** The URL for the http endpoint where the identity provider issues access tokens.
  - ☐ **User Info URI.** The URL for the http endpoint where the identity provider maintains user information. Requests from the client application for additional information about the current user that also include a valid access token are directed to this endpoint.
  - ☐ **Logout URI.** The URL for the http endpoint to which users must be directed when they choose to sign out of their session.
7. Type a valid attribute name in the Attribute Name for User ID field.

**Note:** You will most likely replace the default value, name, with the value, email. However, other attribute names can be used in this field. For more information about the value to use, consult your identity provider.
8. If you must ensure that any user ID submitted to the identity provider excludes a domain name prefix, select the *Strip the Domain Name from User ID* check box. Otherwise, leave this check box clear.

**Note:** This check box is relevant only to customers who use the *domain name\user ID* format for their user names and work with an OpenID Connect identity provider that does not accept user IDs with a domain name prefix.

9. Enter the names of the optional scope identifiers that you and your identity provider have agreed to use in the Optional Scope Values field. Separate each value with a single space.

**Note:** You can clear the value *email* that appears in this field, by default, if you and your identity provider do not support it.

10. Accept the default selection of *HTTP POST* in the Client Authentication Method list or select *HTTP Basic Authentication Scheme* to identify the HTTP communication method required by your identity provider for end user authentication messages.

**Note:** We do not recommend that you select *None* unless required to do so by your identity provider.

11. When your configuration is complete, click *OK*.
12. Enable the new configuration as described in [How to Enable OpenID Connect Authentication in a Security Zone](#) on page 249.
13. Save the new configuration as described in [How to Save an OpenID Connect Configuration](#) on page 250.

### **Procedure:** How to Enable OpenID Connect Authentication in a Security Zone

Only one OpenID Connect provider can be supported per installation.

When OpenID Connect Authentication is enabled in a security zone, all other methods of authentication in that zone must be disabled.

As with other methods of pre-authentication, we recommend using this method in the Default Security Zone while allowing the Alternate Zone to support Form-Based Authentication for administration activities.

1. In the Administration Console, on the Security tab, under the Security Zones folder, expand the *Default Security Zone* folder, and then click *Authentication*.
2. On the Authentication page:
  - a. Click the *Form Based Authentication* entry and then click *Disable*.
  - b. Click the *Anonymous Authentication* entry and then click *Disable*.
  - c. Click the *OpenID Connect Authentication* entry and then click *Enable*.
3. Save the Authentication page with the OpenID Connect configuration as described in [How to Save an OpenID Connect Configuration](#) on page 250.

**Procedure: How to Save an OpenID Connect Configuration**

1. In the Actions section of the Authentication page, click **Save**.
2. When you receive a confirmation message, click **OK**.
3. When you receive a message advising you to reload the web application, click **OK**.
4. Sign out of your current session.
5. Stop and restart the WebFOCUS Reporting Server.
6. Sign in using a valid ID from your OpenID Connect identity provider to test the new configuration.

**Configuring Pre-Authentication With Web Access Management Systems**

Web Access Management Systems, including CA SiteMinder, Oracle Access Manager (formerly Oblix), and IBM Tivoli Access Manager WebSEAL, can be used to enable single sign on (SSO) with WebFOCUS. These systems intercept requests to WebFOCUS, ensure that the user is authenticated and authorized to access WebFOCUS, and then provide an HTTP header in which WebFOCUS can find the pre-authenticated user ID. Because these systems intercept and populate the HTTP header on every request, WebFOCUS can trust that the user ID found in the HTTP header is valid.

**Procedure: How to Configure Pre-Authentication With Web Access Management Systems**

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

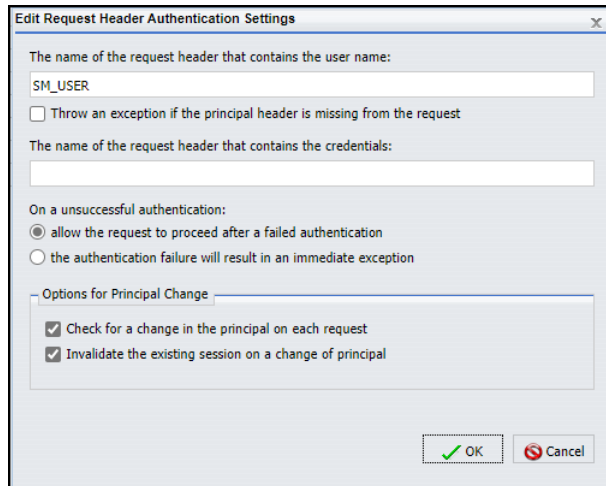
We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

1. In the Administration Console, click the **Security** tab.
2. On the Security tab, under the folder for the Security zone that will support pre-authentication with the Web Access Management System, click **Authentication**.

Typically, this is the Default Security zone.

3. Right-click the Request Header Authentication Entry, and click **Edit**.

4. Type the default name provided by the Web Access Management System in The name of the request header that contains the user name field, as shown in the following image.



- ☐ For CA SiteMinder, the value is typically SM\_USER.
  - ☐ For IBM Tivoli Access Manager WebSEAL, the value is typically iv-user.
  - ☐ For Oracle Access Manager, consult your Oracle Access Manager documentation.
5. Click *OK*.
  6. In the Actions section of the Authentication Page, click *Options*.
  7. In the Authentication Options dialog box, select the *Enable custom logout target URL* check box.
  8. Type the custom logout target URL for your Web Access Management System as provided by the Web Access Management System.
    - ☐ For Siteminder, the value is typically *http://siteminder.domain.com/logout.html*.
    - ☐ For IBM Tivoli Access Manager WebSEAL, the value is typically *http://webseal.domain.com/pkmslogout*.
    - ☐ For Oracle Access Manager, consult Web Access Management documentation or the system administrator.
  9. Click *OK*.
  10. On the Authentication page, right-click *Request Header Authentication* and then click *Enable*.
  11. On the Authentication page, in the Security Zones section, click *Save*.

12. When you receive a message stating that the web security configuration data was saved successfully, click *OK*.
13. When you receive a message advising you to reload the web application in order for these changes to take effect click *OK*.
14. Sign out of your current session.
15. Stop and restart the WebFOCUS Reporting Server.
16. Sign in again as an administrator and test the new configuration.

### **Procedure: How to Configure Request Header Based Authentication**

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

1. In the Administration Console, click the *Security* tab.
2. Under the Security Zones folder, expand the folder for the Security Zone you wish to update and then click *Authentication*.
3. Right-click the *Request Header Authentication* entry, and click *Edit*.
4. In the Edit Request Header Authentication Settings dialog box:
  - a. If you are using CA Site Minder, accept the default name (SM\_USER) as the name of the request header that contains the user name.
  - b. If you are using IBM Tivoli Access Manager WebSEAL, type, iv-user.
  - c. If you are using Oracle Access Manager, type the value provided to you by your Oracle Access Manager Administrator.  
  
The value is case-insensitive, but the spelling must match the spelling of the value in the Administration Console spelling.
5. Leave the *Throw an exception if the principal header is missing from the request* check box cleared, select it only if you want the authentication process to record an exception when this event occurs.
6. In The name of the request header that contains the credentials field, type the User ID.  
  
For example, SM\_USER, iv-user.
7. In the On an unsuccessful authentication section:
  - a. To generate an exception for an unsuccessful authentication, click *the authentication failure will result in an immediate exception*.



- b. To allow the request to proceed in spite of an unsuccessful authentication, accept the default setting, *allow the request to proceed after a failed authentication*.
8. To include a check for a change in user name into each authentication request, select the *Check for a change in the principal on each request* check box.
9. To invalidate a session if the user name changes, select the *Invalidate the existing session on a change in principal* check box.
10. When your configuration is complete, click *OK*.
11. Right-click the Request Header Based Authentication entry, and click *Enable*.
12. In the Actions section, click *Save*.
13. When you receive a message stating that the changes were saved successfully, click *OK*.
14. When you receive a message advising you to reload the web application, click *OK*.
15. Sign out of your current session.
16. Stop and restart the WebFOCUS Reporting Server.
17. Sign in as an administrator, and test the new configuration.

## Configuring Pre-Authentication With Integrated Windows Authentication

In pre-authentication using Integrated Windows Authentication, WebFOCUS uses Microsoft Internet Information Services (IIS) with its Windows Authentication or Basic authentication options to pre-authenticate Microsoft Windows users. This configuration requires a plug-in that enables IIS to securely pass user identities to the JEE web application container that hosts WebFOCUS. Additional information about the configuration of IIS with Tomcat and IIS with WebSphere is included at the end of the following procedure.

### **Procedure:** How to Configure Pre-Authentication With Windows Authentication

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

We also recommend that you enable the Alternate Security Zone when using Windows Authentication to continue support for form-based Internal Authentication of those administrators who must bypass Windows Authentication for administrative tasks. For more information, see [How to Enable a Security Zone](#) on page 154.

1. In the Administration Console, click the *Security* tab.

2. Under the Default Security Zones folder, click *Authentication*.
3. In the Actions section of the Authentication Page, click *Options*.
4. In the Authentication Options dialog box, select the *Enable custom logout target URL* check box, accept the default value */signout* in the Custom logout target URL field, and click *OK*.
5. On the Authentication page, click *JEE Container Based Authentication*.

Typically, IIS prepends the name of the Windows Domain to which the user is assigned to the user ID passed to WebFOCUS, using the domain name\user ID format. By default, WebFOCUS strips the domain and backslash (\) from the value, leaving just the user ID, which is then used to complete the sign-in process.

We recommend that you accept this default behavior, and move to the following step without altering it. If you must modify it, open the *Edit JEE Container Based Authentication Settings* dialog box, clear the *Strip the Domain Name from JEE User Principal Name* check box, and click *OK* to save the change.

6. With the JEE Container Based Authentication entry highlighted, click *Enable*.  
All other methods of authentication are disabled automatically.
7. On the Authentication page, in the Security Zones section, click *Save*.
8. When you receive a message stating that the web security configuration data was saved successfully, click *OK*.
9. When you receive a message advising you to reload the web application, click *OK*.
10. Sign out of your current session.
11. Enable the JEE container to trust the user ID passed by the connector.

- ☐ For Tomcat, open the server.xml file located at *drive:\tomcat\conf* in Windows or *installdirectory/tomcat/conf* in UNIX or Linux, add the tomcatAuthentication keyword in the AJP Connector block, and set it to false, as shown in the following example:

```
<!-- Define an AJP 1.3 Connector on port 8009 -->  
<Connector port="8009" protocol="AJP/1.3"  
tomcatAuthentication="false" redirectPort="8443" />
```

- ☐ For WebSphere, consult the WebSphere documentation for instructions on using the WebSphere REMOTE\_USER variable to expose the user ID that the IIS connector passes to WebFOCUS.
12. Stop and restart the WebFOCUS Reporting Server.

13. Sign in again as an administrator and test the new configuration.

- ❑ If you enabled the alternate zone, as recommended, you can now use internal authentication to access WebFOCUS when signing in to the WebFOCUS machine. The URL is `http://localhost/ibi_apps`. Alternatively, pre-authentication allows you to access WebFOCUS by signing in to `http://machinename/ibi_apps` from any workstation. If the web browser is not configured to use Windows Authentication with the domain automatically, the browser will challenge users for credentials when they sign in using `http://machinename.domain.com/ibi_apps`.
- ❑ By default, Internet Explorer automatically uses Windows Authentication only with website addresses in the form `http://machinename`. To enable Windows Authentication for users who access WebFOCUS by `http://machinename.domain.com`, you may need to reconfigure the local intranet zone settings on the Internet Explorer browsers assigned to user machines.

## Configuring Pre-Authentication With Custom Single Sign On (SSO) Solutions

WebFOCUS can be integrated with other applications to provide users with a single sign on (SSO) experience. For example, users may sign in to an existing web application with credentials that are validated by the application. If users click on buttons or links that take them to a portal, you may want them to be signed in to WebFOCUS automatically, rather than requiring them to provide their passwords again.

The best way to accomplish this sort of integration is through the deployment of a custom Java servlet filter inside the WebFOCUS web application. Professional Services team members can develop a custom solution based on the `IBIServletFilter`. Alternatively, if your users access WebFOCUS through IIS, you can install an HTTP module using ASP.NET into IIS.

Custom solutions generally follow the Shared Secret approach. In this approach, a user initiates a connection to WebFOCUS by clicking a link, button, or tab in the existing web application. The web application sets the user ID, and creates an AES-encrypted token containing the user ID and a timestamp. The web application then passes the token on to WebFOCUS.

Within WebFOCUS, the `IBIServletFilter` decrypts the token and then compares the timestamp to the current time to determine if the token has exceeded a specified interval. The `IBIServletFilter` performs this time check to ensure that a replay attack, that is, a fraudulent attempt to authenticate an unauthorized user based on an outdated token, has not occurred.

If the token has not exceeded the specified interval, the IBIServletFilter compares the user ID from the token to the user ID it maintains. If they match, the user ID is trusted. If they do not match, the connection is rejected.

## Configuring Kerberos for Single Sign On

WebFOCUS supports single sign on (SSO) between a web browser, the WebFOCUS Client, and the WebFOCUS Reporting Server in networks that use Kerberos pre-authentication. This includes impersonation support on the WebFOCUS Reporting Server, which means that the SSO capability can be extended through RDBMS adapters that support trusted connections, including Microsoft SQL Server.

This topic explains how to configure WebFOCUS within an SSO environment that uses native Kerberos support in Active Directory. This activity requires updates to Windows Active Directory, WebFOCUS, and the browsers assigned to it. Active Directory must be configured to include accounts for the servers that support the WebFOCUS Client and the WebFOCUS Reporting Server and to define the method of delegation for Kerberos credentials. WebFOCUS must be configured to support Kerberos authentication for each relevant security zone. Individual browsers assigned to users must be configured to identify the server and client URLs that support the use of Kerberos authentication. These tasks are described in detail in this topic.

## Limitations on Pre-authentication Using Kerberos

- ❑ **ReportCaster.** You can use ReportCaster in a Kerberos environment. For configuration details and additional release level requirements, see [Configuring Support for ReportCaster for Kerberos](#) on page 294.
- ❑ **WebFOCUS Client and WebFOCUS Reporting Server on the same machine.** When both components are on one machine, you must specify the HOST keyword for the node in computer name format. Using localhost or a fully qualified domain name results in run-time errors. If the components are on different machines, you can use either computer name format or fully qualified domain name format. The HOST keyword is specified in the Remote Services section of the Administration Console.
- ❑ **Web browser.** Kerberos is not supported between a web browser and WebFOCUS when the two are on the same Windows machine.
- ❑ **Users who belong to many groups.** The Kerberos implementation stores each group that a user belongs to inside their Kerberos ticket. This can result in large ticket sizes when users belong to hundreds of groups. For configuration details, see [Configuring Support for Large Tickets for Kerberos](#) on page 295.

- ❑ **User ID format.** When using Kerberos pre-authentication, you must create WebFOCUS user IDs that match the IDs in the credentials that Kerberos assigns to individual users. Kerberos typically appends the Windows Domain of a user to the ID for that user, but WebFOCUS is configured to strip this domain, by default. Therefore, for most organizations, the Kerberos user ID, without the domain suffix, is all that is required as a WebFOCUS user ID.

However, if your organization has disabled this default configuration, user IDs must use the format:

*user\_ID @ domain.com*

where:

*user\_ID*

Is the appropriate user ID passed to WebFOCUS in the Kerberos ticket.

*domain.com*

Is an available domain and extension.

- ❑ **Domain suffix.** Generally, when Kerberos passes a user ID to WebFOCUS, it appends the Windows Domain of that user to the ID itself, in the format *user ID@domain.com*. By default, the domain is stripped from this concatenated value, leaving just the user ID. The plain user ID that remains is then used to complete the sign-in process.

To override this default configuration and prevent WebFOCUS from stripping the domain, clear the Enable Domain Name Suffix Stripping check box in the EDIT KERBEROS/SPNEGO dialog box, which opens from the Authentication Page on the Security tab of the Administration Console.

## Understanding Constrained Delegation Versus Unconstrained Delegation

WebFOCUS can support unconstrained delegation and constrained delegation of account credentials granted by Kerberos pre-authentication.

Unconstrained delegation allows account credentials to be delegated to any service in the domain. Constrained delegation limits delegation of account credentials to a specified list of services.

The configuration for either method follows the same basic path. However, in order to establish constrained delegation to the WebFOCUS Reporting Server alone or to the WebFOCUS Reporting Server and the Database Server, you must add the following configuration tasks:

- ☐ Identify the machines to which accounts are to be delegated with Service Principal Names (SPN).
- ☐ Specify HTTP as the Service Type and identify the specific computer to which Kerberos authentication is to be delegated.

If you must also delegate Kerberos authentication from the WebFOCUS Reporting Server to a relational database management server (RDBMS), you must configure a connection that supports this delegation on the WebFOCUS Reporting Server. For more information, see the *Kerberos configuration and testing procedures* content assigned to the Reporting Server browser interface Help.

### Pre-Installation Steps for Kerberos in Windows Active Directory

The pre-installation steps required to include WebFOCUS in Windows Active Directory vary, depending upon whether you use constrained delegation of Kerberos credentials or unconstrained delegation.

If you use constrained delegation, a network administrator with Domain Administration privileges must perform the following pre-installation steps.

- ☐ Ensure that a Service Principal Name (SPN) is available for the WebFOCUS Reporting Server.
- ☐ Create a service account in Active Directory for the WebFOCUS Client.
- ☐ Generate a Kerberos keytab file for the WebFOCUS Client, using the ktpass command in the KTPASS.EXE utility.
- ☐ Configure the Service User Account in Active Directory for constrained delegation.

If you use unconstrained delegation, a network administrator with Domain Administration privileges must perform the following pre-installation steps.

- ☐ Create a service account in Active Directory for the WebFOCUS Client.
- ☐ Generate a Kerberos keytab file for the WebFOCUS Client, using the ktpass command in the KTPASS.EXE utility.
- ☐ Configure the Service User Account in Active Directory for unconstrained delegation.

**Note:** In either case, if you are running Windows 2008, you may need to install the following Microsoft patch for your domain controller to support the use of a Kerberos keytab file:

<http://support.microsoft.com/kb/951191>

### **Procedure:** How to Check for a Service Principal Name (SPN) on the WebFOCUS Reporting Server

If you choose to use unconstrained delegation of Kerberos credentials, you do not need a Service Principal Name for the WebFOCUS Reporting Server and can bypass this procedure. Continue with the procedure, [How to Create a Service Account User in Windows Active Directory](#) on page 263.

If you choose to use constrained delegation of Kerberos credentials, you must have a Service Principal Name (SPN) for the WebFOCUS Reporting Server before you can delegate Kerberos credentials to it. You can use this procedure to identify the SPN that has been assigned to the WebFOCUS Reporting Server.

However, if you already know the SPN for the WebFOCUS Reporting Server, you can bypass this procedure and move on to [How to Create a Service Account User in Windows Active Directory](#) on page 263.

1. On the domain controller or another machine that is logged on to the Windows domain, log on as a domain administrator, and then open the Command Prompt window.
2. Type and run the following command to determine if a Service Principal Name was created for the machine that hosts the WebFOCUS Reporting Server:

```
setspn -l hostname
```

where:

*hostname*

Is the machine name for the WebFOCUS Reporting Server. For example, rs-kerb.

3. If the resulting output returns the message

```
Could not find account hostname
```

where:

*hostname*

Is the machine name for the WebFOCUS Reporting Server. For example, rs-kerb.

The WebFOCUS Reporting Server was not added to the domain.

For information about how to add a WebFOCUS Reporting Server to a domain, see the procedure, [Adding Users and Computers to the Active Directory Domain](#) at <https://support.microsoft.com/en-us/help/324753/how-to-create-an-active-directory-server-in-windows-server-2003>.

4. If the resulting output returns the message

`Registered ServicePrincipalName...`

but does *not* include the entry:

`HTTP/hostname.ibi.com`

where:

`hostname.ibi.com`

Is the full SPN name for the WebFOCUS Reporting Server, with *hostname* being the machine name for the WebFOCUS Reporting Server, for example, rs-kerb.ibi.com.

An SPN that will support constrained delegation is not available for the WebFOCUS Reporting Server.

You must create a new SPN for the WebFOCUS Reporting Server as described in the procedure, [How to Create a Service Principal Name \(SPN\)](#) on page 261.

5. If the resulting output returns the message:

`Registered ServicePrincipalName...`

and includes the entry:

`HTTP/hostname.ibi.com`

where:

`hostname.ibi.com`

Is the full SPN name for the WebFOCUS Reporting Server, with *hostname* being the machine name for the WebFOCUS Reporting Server, for example, rs-kerb.ibi.com.

An SPN that will support constrained delegation is available for the WebFOCUS Reporting Server.

Continue with the topic, [How to Create a Service Account User in Windows Active Directory](#) on page 263.



## Examples of Check Service Principal Name (SPN) Results

The following example of a successful result identifies the Service Principal Names for a WebFOCUS Reporting Server named rs-kerb. The second line identifies HTTP/rs-kerb.ibi.com as the full SPN for that WebFOCUS Reporting Server.

```
setspn -l rs-kerb
Registered ServicePrincipalNames for CN=RS-KERB, OU=Workstations,DC=ibi,DC=com:
    HTTP/rs-kerb.ibi.com
    TERMSRV/rs-kerb.ibi.com
    TERMSRV/RS-KERB
    WSMAN/rs-kerb.ibi.com
    WSMAN/rs-kerb
    RestrictedKrbHost/rs-kerb.ibi.com
    RestrictedKrbHost/RS-KERB
    HOST/RS-KERB
    HOST/rs-kerb.ibi.bom
```

The following example of an unsuccessful result contains a message stating that the setspn statement was unable to find an account with the name rs-kerb.

```
setspn -l rs-kerb
FindDomainForAccount: Call to DsGetDcNameWithAccountW failed with return
value 0x00000525
Could not find account rs-kerb
```

### **Procedure:** How to Create a Service Principal Name (SPN)

Use the setspn command to create a Service Principal Name (SPN) for the WebFOCUS Reporting Server.

1. On the domain controller or another machine that is logged on to the Windows domain, log on as a domain administrator, and then open the Command Prompt window.
2. Type and run the following command.

**Note:** The value specified for the full SPN name for the WebFOCUS Reporting Server must begin with HTTP in uppercase, followed by a slash ( / ).

The command format is:

```
setspn -a HTTP/hostname.ibi.com hostname
```

where:

*hostname.ibi.com*

Is the full SPN name for the WebFOCUS Reporting Server, with *hostname* being the machine name for the WebFOCUS Reporting Server, for example, rs-kerb.ibi.com.

The resulting output is:

```
Registering ServicePrincipalNames for CN=hostname,  
CN=Computers,DC=ibi,DC=com  
    HTTP/hostname.ibi.com  
Updated object
```

where:

*hostname*

Is the computer name for the WebFOCUS Reporting Server, with *hostname* being the machine name for the WebFOCUS Reporting Server, for example, rs-kerb.ibi.com.

3. Confirm the presence of the newly-created SPN by typing and running the following command:

```
setspn -l hostname
```

where

*hostname*

Is the new SPN you just created. For example, rs-kerb.

If your results were successful, you should see the following message:

```
Registered ServicePrincipalNames for  
CN=hostname,CN=Computers,DC=ibi,DC=com
```

followed by a list of results that includes the entry:

```
HTTP/hostname.ibi.com
```

where:

*hostname.ibi.com*

Is the new SPN you just created, with *hostname* being the machine name for the WebFOCUS Reporting Server, for example, rs-kerb.ibi.com. This is the only value that is relevant to Kerberos delegation.

### Examples of a Successful Service Principal Name (SPN) Registration

The following example of a successful Service Principal Name registration identifies HTTP/rs-kerb.ibi.com as the new Service Principal Name for the computer name rs-kerb.

```
Registering ServicePrincipalNames for CN=RS-KERB,CN=Computers,DC=ibi,DC=com  
    HTTP/rs-kerb.ibi.com  
Updated object
```

The following example of a response message confirms the presence of the newly-created SPN by listing all of the Registered Service Principal Names for the computer name rs-kerb:

```
Registered ServicePrincipalNames for CN=RS-KERB,CN=Computers,DC=ibi,DC=com:
HTTP/rs-kerb.ibi.com
WSMAN/rs-kerb
WSMAN/rs-kerb.ibi.com
TERMSRV/RS-KERB
TERMSRV/rs-kerb.ibi.com
RestrictedKrbHost/RS-KERB
HOST/RS-KERB
RestrictedKrbHost/rs-kerb.ibi.com
```

### **Procedure: How to Create a Service Account User in Windows Active Directory**

This procedure creates a service account in Active Directory for the WebFOCUS SSO feature. It identifies the WebFOCUS Client in Kerberos operations.

1. On the domain controller, open the Windows Active Directory Users and Computers Window.
2. Navigate to the folder that will contain the new user, and open it.
3. Right-click anywhere in the user list, and then click *New User*.
4. On the first page of the New Object - User wizard, type the name of the machine on which WebFOCUS is installed in the First name field and in the Full name field, as shown in the following image.



The screenshot shows the 'New Object - User' wizard. At the top, it says 'Create in: ibi.com/COR/BIPG/DEVELOPMENT/USERS'. Below this, there are three input fields: 'First name' with the value 'http\_wf-kerb', 'Last name' which is empty, and 'Full name' with the value 'http\_wf-kerb'. There is also an 'Initials' field which is empty.

The value specified for the First name and Full name must begin with http in lowercase letters, followed by an underscore character (\_). The format is:

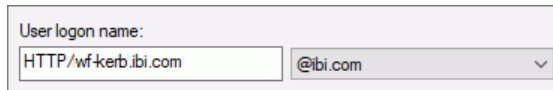
*http\_hostname*

where:

*hostname*

Is the computer name of the machine on which the WebFOCUS Client is installed. For example, wf-kerb.

5. Type the name of the machine on which the WebFOCUS Client is installed in the User logon name field, as shown in the following image.



The image shows a form with the label "User logon name:". Below it is a text input field containing "HTTP/wf-kerb.ibi.com" and a dropdown menu showing "@ibi.com".

The value specified for the User logon name must begin with HTTP in uppercase, followed by a slash (/). The format is:

*HTTP/hostname.domain.ext*

where:

*hostname.domain.ext*

Is the fully qualified domain name of the machine on which the WebFOCUS Client is installed.

6. Type over the automatically-assigned value in the User logon name (pre-Windows 2000) text box with the name of the machine on which the WebFOCUS Client is installed, as shown in the following image.



The image shows a form with the label "User logon name (pre-Windows 2000):". Below it is a text input field containing "http\_wf-kerb" and a dropdown menu showing "IBI\".

The value specified for the User logon name must begin with http in lowercase followed by an underscore (\_). The format is:

*http\_hostname*

where:

*hostname*

Is the name of the machine on which the WebFOCUS Client is installed. For example, wf-kerb.

The value specified for the User logon name (pre-Windows 2000) becomes the SAMAccountName attribute for the service account.

7. Review your input, as shown in the following image, and then click *Next*.

In this example, the New Object - User dialog box contains values in the recommended format, indicating that the WebFOCUS Client is installed on a machine named wf-kerb.

New Object - User

Create in: ibi.com/COR/BIPG/DEVELOPMENT/USERS

First name: http\_wf-kerb Initials:

Last name:

Full name: http\_wf-kerb

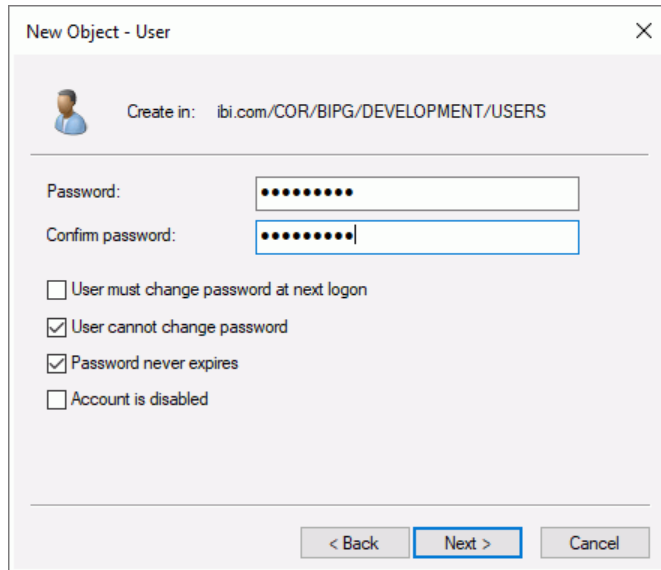
User logon name: HTTP/wf-kerb.ibi.com @ibi.com

User logon name (pre-Windows 2000): IBI\ http\_wf-kerb

< Back Next > Cancel

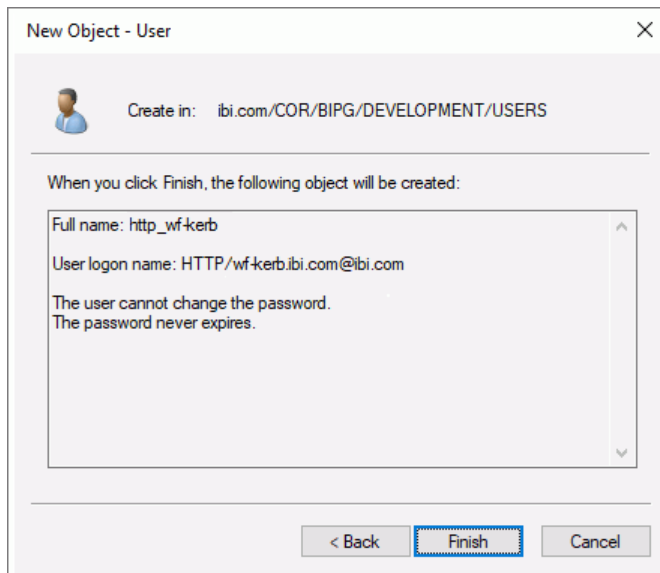
8. When the second page opens and prompts you for the password, as shown in the following image, do the following:
  - a. Type a password for the service account user in the Password and Confirm password fields.
  - b. Clear the *User must change password at next logon* check box.

- c. Select the *User cannot change password* and *Password never expires* check boxes, and then click *Next*.



The 'New Object - User' dialog box shows the 'Create in' path as ibi.com/COR/BIPG/DEVELOPMENT/USERS. It has two password fields, both filled with dots. Below them are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (checked), 'Password never expires' (checked), and 'Account is disabled' (unchecked). At the bottom are '< Back', 'Next >', and 'Cancel' buttons. The 'Next >' button is highlighted with a blue border.

9. When the confirmation page opens, review the list of properties for the service account user that will be created, as shown in the following image, and then click *Finish*.



The 'New Object - User' dialog box shows the 'Create in' path as ibi.com/COR/BIPG/DEVELOPMENT/USERS. It contains a text area with the following text: 'When you click Finish, the following object will be created:', 'Full name: http\_wf-kerb', 'User logon name: HTTP/wf-kerb.ibi.com@ibi.com', 'The user cannot change the password.', and 'The password never expires.' At the bottom are '< Back', 'Finish', and 'Cancel' buttons. The 'Finish' button is highlighted with a blue border.

**Procedure: How to Run the ktpass Command for the Service Account User**

In order to set the servicePrincipalName (SPN) attribute on your service account and to generate the Kerberos keytab file for WebFOCUS, you must run the ktpass command from the Command Prompt window of the domain controller. Type the command and all arguments and values on a single line. We recommend that you keep a copy of the command syntax you use to support troubleshooting later.

1. On the domain controller, open the Command Prompt window.
2. In the Command Prompt window, type the ktpass command using the following format:

```
ktpass /out filename /mapuser user_ID /princ principal /crypto
encryption /pass password /ptype KRB5_NT_PRINCIPAL
```

where:

*filename*

Is the name that ktpass will use to create the Kerberos keytab file. The recommended value is http\_hostname.keytab.

where:

*hostname*

Is the full name of the WebFOCUS Client Service Account. For example, wf-kerb.ibi.com.

*user\_ID*

Is the sAMAccountName value provided in the User logon name (pre-Windows 2000) field of the Service Account.

*principal*

Is specified by concatenating the user logon name value provided in the User logon name field of the Service Account with @REALM, where REALM is the Kerberos realm. The Kerberos realm generally uses the same value as the Active Directory DNS suffix, except that the Kerberos realm is typed in uppercase characters.

*encryption*

Is the encryption option that will be used when creating the keytab file. You may need to download the latest Microsoft support tools for a version of the ktpass command that supports the recommended value of All.

**Note:** If any of the machines on your network are running Windows 2008 R2, Windows 7, or later, you must choose All for these machines to function properly with Kerberos. Microsoft removed all support for DES in later versions of Windows.

*password*

Is the Windows password associated with the service account, in plain text.

The following example shows a correctly-formatted ktpass command that applies to the examples provided previously in this section:

```
C:\>ktpass /out http_wf-kerb.keytab /mapuser http_wf-kerb /princ
HTTP/wf-kerb.ibi.com@IBI.COM /crypto All /pass password1
/ptype KRB5_NT_PRINCIPAL
```

3. If the ktpass command is successful, the Command Prompt window displays the Successfully mapped response message, as shown in the following example.

```
Targeting domain controller: ibidca.ibi.com
Successfully mapped HTTP/wf-kerb.ibi.com to http_wf-kerb.
Key created.
Output keytab to http_wf-kerb.keytab:
Keytab version: 0x502
keysize 63 HTTP/wf-kerb.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 2 etype
0x17 (RC4-HMAC) keylength 16 (0x0df97e7355555817c828671454137af0)
```

4. Open a utility that allows you to view Active Directory Service Account properties and open the properties for the new Service Account.

Scroll through the property names to confirm that the ktpass command added an attribute named servicePrincipalName (SPN) and modified the sAMAccountName and the userPrincipalName (UPN) attributes, as shown in the following image.

Name	Value	Type
name	http_wf-kerb	Attribute
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=ibi,DC=...	Attribute
objectClass	user	Attribute
objectClass	top	Attribute
objectClass	person	Attribute
objectClass	organizationalPerson	Attribute
primaryGroupID	513	Attribute
pwdLastSet	1/10/2018 3:32:47 PM	Attribute
sAMAccountName	http_wf-kerb	Attribute
sAMAccountType	< samUserAccount >	Attribute
servicePrincipalName	HTTP/wf-kerb.ibi.com	Attribute
userAccountControl	[ NormalAccount, NoPasswordExpiration ]	Attribute
userPrincipalName	HTTP/wf-kerb.ibi.com@IBI.COM	Attribute



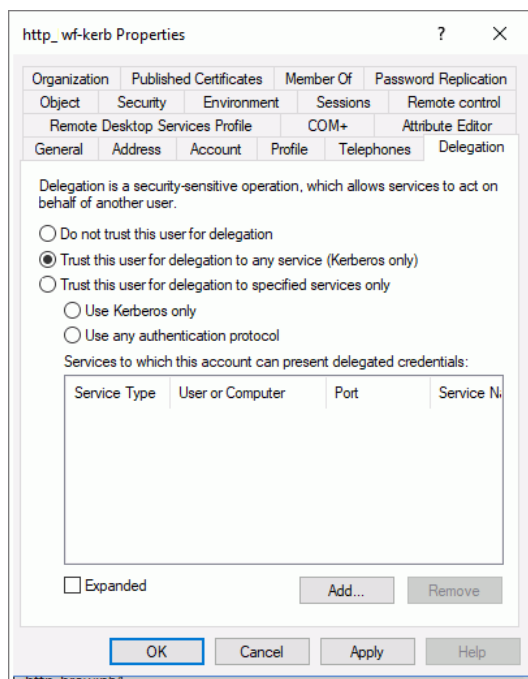
### **Procedure:** How to Configure the Service Account User in Active Directory for Delegation

You can configure constrained delegation or unconstrained delegation for Kerberos in the Windows Active Directory by using the Delegation tab in the Properties dialog box for the Service Account User.

1. In the Active Directory Users and Computers Window Users list, right-click the service account user, and then click *Properties*.
2. In the Properties dialog box, click the *Delegation* tab.

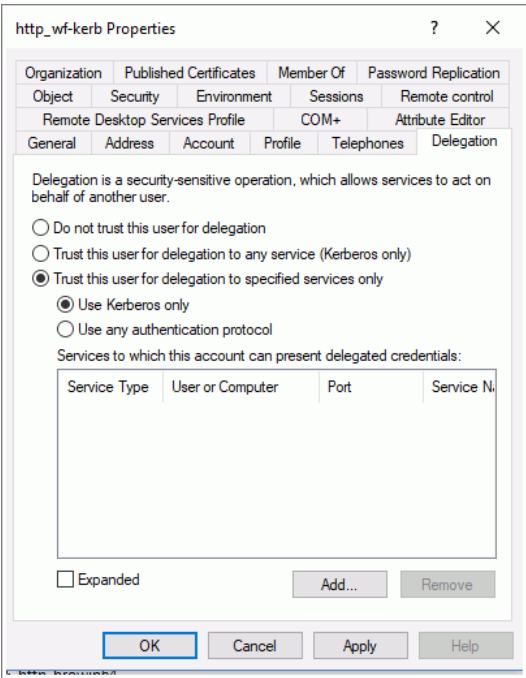
**Note:** The Delegation tab appears only after you run the ktpass command. For more information, see [How to Run the ktpass Command for the Service Account User](#) on page 267.

3. If you want to use unconstrained delegation, accept the default selection of the *Trust this user for delegation to any service (Kerberos only)* option, as shown in the following image, and continue with step 9.

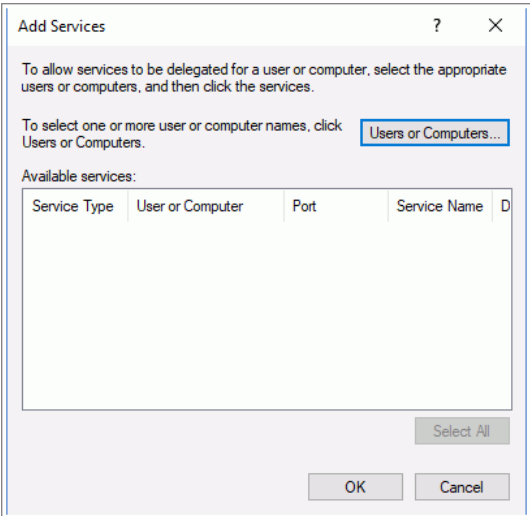


- 4. If you want to use constrained delegation, click *Trust this user for delegation to specified services only* and then click *Add*, as shown in the following image.

**Note:** The Use Kerberos only option is selected, by default



- 5. In the Add Services dialog box, click *Users or Computers*, as shown in the following image.



- In the Select Users or Computers dialog box, type the SPN name of the service to which this account can present delegated credentials in the Enter the object names to select text box, as shown in the following image, and then click *OK*.

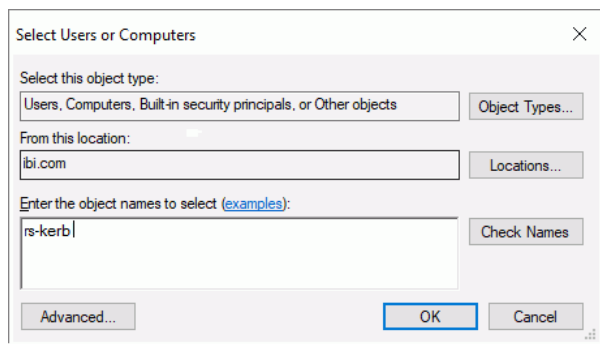
Typically this value is:

*hostname*

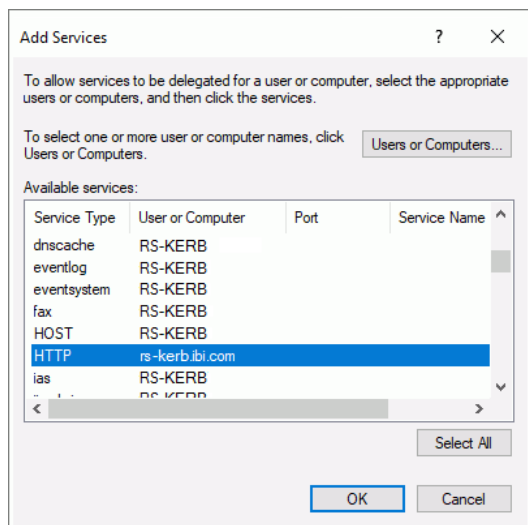
where:

*hostname*

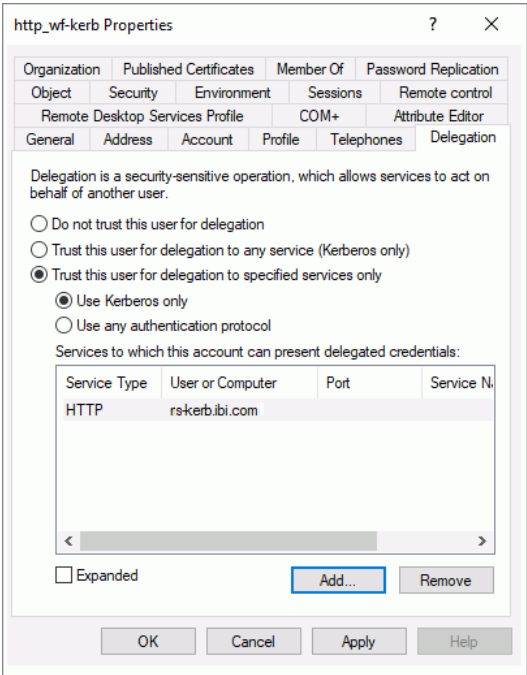
Is the SPN name for the WebFOCUS Reporting Server to which this account can present delegated credentials.



- In the Add Services dialog box, click *HTTP*, in the Available Services list Service Type column, as shown in the following image, and then click *OK*.



- 8. Confirm that the Service Type and Service Account Name appear in the Services to which this account can present delegated credentials list, as shown in the following image, and then click OK



- 9. If you are not using host headers, copy the resulting keytab file (for example, http\_wf-kerb.keytab) to the machine on which you will install WebFOCUS. If you are using host headers, continue with [Host Header Support for Kerberos](#) on page 272.

Host Header Support for Kerberos

If you are using one or more host headers, you must perform the following steps.

**Procedure:** How to Implement Host Header Support for Kerberos

The following procedure assumes that there are two host header names, which are wf-kerb1 and wf-kerb2.

- 1. Add A records for each host header in DNS, pointing to the same IP address as the NetBIOS name.

**Note:** Do not create C records.

- 2. Run a ktpass command for each host header, using the following format:

```
ktpass /in filename /out filename /princ principal /crypto encryption/
pass password /ptype KRB5_NT_PRINCIPAL
```

- a. For wf-kerb1, run the following ktpass command:

```
ktpass /in c:\keytab\http_wf-kerb.keytab
/out c:\keytab\http_wf-kerb.keytab
/princ HTTP/wf-kerb1.ibi.com@IBI.COM /crypto All
/pass password1 /ptype KRB5_NT_PRINCIPAL
```

The resulting output is:

```
Existing keytab:
Keytab version: 0x502
keysize 63 HTTP/wf-kerb.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 2 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
NOTE: creating a keytab but not mapping principal to any user.
      For the account to work within a Windows domain, the
      principal must be mapped to an account, either at the
      domain level (with /mapuser) or locally (using ksetup)
      If you intend to map HTTP/wf-kerb1.ibi.com@IBI.COM to an
      account through other means or don't need to map the
      user, this message can safely be ignored.
WARNING: pType and account type do not match. This might cause
problems.
Key created.
Output keytab to c:\keytab\http_wf-kerb.keytab:
Keytab version: 0x502
keysize 63 HTTP/wf-kerb.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 2 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
keysize 64 HTTP/wf-kerb1.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 1 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
```

- b. For wf-kerb2, run the following ktpass command:

```
ktpass /in c:\keytab\http_wf-kerb.keytab
/out c:\keytab\http_wf-kerb.keytab
/princ HTTP/wf-kerb2.ibi.com@IBI.COM /crypto All
/pass password1 /ptype KRB5_NT_PRINCIPAL
```

The resulting output is:

```
Existing keytab:
Keytab version: 0x502
keysize 63 HTTP/wf-kerb.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 2 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
keysize 64 HTTP/wf-kerbl.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 1 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
NOTE: creating a keytab but not mapping principal to any user.
      For the account to work within a Windows domain, the
      principal must be mapped to an account, either at the
      domain level (with /mapuser) or locally (using ksetup)
      If you intend to map HTTP/wf-kerb2.ibi.com@IBI.COM to an
      account through other means or don't need to map the
      user, this message can safely be ignored.
WARNING: pType and account type do not match. This might cause
problems.
Key created.
Output keytab to c:\keytab\http_wf-kerb.keytab:
Keytab version: 0x502
keysize 63 HTTP/wf-kerb.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 2 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
keysize 64 HTTP/wf-kerbl.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 1 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
```

### 3. Run the following setspn commands.

**Note:** You can refer to each host header in two ways, either by using the fully qualified domain name or by using the one-part name. For example, you can refer to the first host header as wf-kerb1.ibi.com (fully qualified domain name) or as wf-kerb1 (one-part name). As a result, when you run the setspn commands in this step, there are four entries.

#### a. Run:

```
setspn -A HTTP/wf-kerbl.ibi.com ibi\http_wf-kerb
```

The resulting output is:

```
Registering ServicePrincipalNames for CN=http_wf-
kerb,OU=USERS,OU=DEVELOPMENT,
O=BIPG,OU=COR,DC=ibi,DC=com
      HTTP/wf-kerbl.ibi.com
Updated object
```

#### b. Run:

```
setspn -A HTTP/wf-kerb1 ibi\http_wf-kerb
```

The resulting output is:

```
Registering ServicePrincipalNames for CN=http_wf-
kerb,OU=USERS,OU=DEVELOPMENT,
O=BIPG,OU=COR,DC=ibi,DC=com
    HTTP/wf-kerb1
Updated object
```

c. Run:

```
setspn -A HTTP/wf-kerb2.ibi.com ibi\http_wf-kerb
```

The resulting output is:

```
Registering ServicePrincipalNames for CN=http_wf-
kerb,OU=USERS,OU=DEVELOPMENT,
O=BIPG,OU=COR,DC=ibi,DC=com
    HTTP/wf-kerb2.ibi.com
Updated object
```

d. Run:

```
setspn -A HTTP/wf-kerb2 ibi\http_wf-kerb
```

The resulting output is:

```
Registering ServicePrincipalNames for CN=http_wf-
kerb,OU=USERS,OU=DEVELOPMENT,
O=BIPG,OU=COR,DC=ibi,DC=com
    HTTP/wf-kerb2
Updated object
```

## TIBCO WebFOCUS Reporting Server Configuration Requirements for Kerberos Constrained Delegation

If you want to use unconstrained delegation with Kerberos pre-authentication, disregard this section. This configuration is not relevant to unconstrained delegation.

- ☐ If you want to use constrained delegation with Kerberos pre-authentication, you must specify Kerberos as the connection type and configure the WebFOCUS Reporting Server to run with Operating System Security.
- ☐ If the WebFOCUS Reporting Server runs on the Windows Operating system, you must configure it to run with Operating System Security.
- ☐ If the WebFOCUS Reporting Server runs on UNIX or Linux, you must configure it to run with the OPSYS security provider. For more information, see the *TIBCO WebFOCUS® Reporting Server Administration* technical content.

## TIBCO WebFOCUS Client Configuration Steps for Kerberos

The following procedure describes the steps for configuring the WebFOCUS Client for Kerberos pre-authentication.

The Default zone, the Portal Zone, and the Alternate Zone can support Kerberos pre-authentication. However, if you use the Alternate Zone for local administrative access, you must not configure it for Kerberos pre-authentication because Kerberos cannot support authentication when the WebFOCUS Client and the browser are installed on same machine.

When created during the installation process, the administrative user is not typically assigned a valid Kerberos User ID. Therefore, in the first part of the configuration, you replace the existing administrative user with a new administrative user to whom you assign a valid Kerberos User ID. WebFOCUS can then manage Kerberos pre-authentication and all other authentication tasks with this new administrative user.

The ID that you assign to the administrative user, and to all users that are subject to Kerberos pre-authentication, must follow the format conventions for Kerberos User IDs that are established in your product installation. By default, WebFOCUS strips domains from the names of all Kerberos User IDs. If you accept this default configuration, you only need to assign a name to the ID of the administrative user or any other user subject to Kerberos pre-authentication. However, if you deactivate this feature by clearing the Enable Domain Name Suffix Stripping check box in the Edit KERBEROS/SPNEGO Authentication Settings dialog box, User IDs must also include the domain to which the user is assigned as well as the name, and they must follow the required format User ID@domain.com.

For more information about Kerberos user names and their format requirements, see [Limitations on Pre-authentication Using Kerberos](#) on page 256.

In the second part of the configuration, you identify the name or location of following items:

- ☐ Service principal name
- ☐ The location of the KeyTab
- ☐ The location of the krb5.conf Configuration File

Each of these items represents the name or location of a key component of the Kerberos pre-authentication method, and all of them are required.

**Note:** The krb5 configuration file is named krb5.ini in Windows or krb5.conf in UNIX.



In order to assign these values to the Security Zone that supports Kerberos pre-authentication, you must type them in the Edit KERBEROS/SPNEGO Authentication settings dialog box, which is located on each of the Security Zone-based Authentication pages of the Administration Console Security tab. Settings for the Default Security Zone, are stored in the securitysettings.xml file. Settings for the Alternate Security Zone are stored in the securitysettings-zone.xml file. Settings for the Portal Zone are stored in the securitysettings-portlet.xml file.

**Procedure: How to Create an Administrative User for Kerberos Pre-Authentication**

In this procedure you create an account for the administrative user that will replace the default administrator once you convert WebFOCUS from internal authentication to Kerberos pre-authentication.

1. Sign in as an administrator.
2. Open the *Security Center*.
3. In the Users pane, under the Users folder, click *New User*.
4. Type the ID of a valid Kerberos user in the Name field, using one of the following formats:
  - ☐ Type only the User ID if your Kerberos configuration automatically strips domains from User IDs.
  - ☐ Type the User ID and Domain of the administrative user in the Name field, using the format User ID@domain.com, if your Kerberos configuration does not automatically strip domains from User IDs.
5. In the Create in Group list, click *Administrators*, and then click *OK*.
6. In the Users pane, under the Users folder, click the previously-created Administrative User, and then click *Delete*.
7. Navigate away from the security center.

**Procedure: How to Configure the TIBCO WebFOCUS Client for Kerberos**

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

1. Open the *Administration Console*.
2. Click the *Security* tab.

3. Under the Security Zones folder, expand the folder for the Security Zone you wish to update, and then click *Authentication*.
4. Double-click the *KERBEROS/SPNEGO Authentication* entry.

or

Click the *KERBEROS/SPNEGO Authentication* entry, and then, in the Actions section, click *Edit*.

or

Right-click the *KERBEROS/SPNEGO Authentication* entry, and then click *Edit*.

5. In the Edit KERBEROS/SPNEGO Authentication settings dialog box:
  - a. Type the Kerberos Service Principal name in the Service principal name field.  
For example, *HTTP/wf-kerb.ibi.com*.
  - b. Type the location of the keytab file in The location of the KeyTab field.

We recommend that you place this file in the config directory.

For example:

*drive:/ibi/WebFOCUS82/config/http\_wfkerb.keytab*

where:

*drive*

Is the letter of the drive that hosts the WebFOCUS application.

- c. Type the location of the krb5 configuration file in *The location of the krb5.conf Configuration File* field.

We recommend that you place this file in the config directory.

For example:

*drive:/ibi/WebFOCUS82/config/krb5configfilename*

where:

*drive*

Is the letter of the drive that hosts the WebFOCUS application.

*krb5configfilename*

Is krb5.ini in Windows or krb5.conf in UNIX.

**Note:** All of these values are required. These examples represent the typical values for each attribute. If your organization uses a different Kerberos Service provider name, or has placed any of the other components in a different location, type that name or location in these fields instead of the name or location called for in the preceding sub-steps.

- d. Accept the default selection of the *Enable Domain Name Suffix Stripping* check box and the *Enable Fallback to Form Authentication* check box.

When this second check box is selected, Form Based Authentication is also enabled in this Security Zone as a supplemental method of authentication if Kerberos fails.

- e. Click *OK*.

- 6. Right-click the *KERBEROS/SPNEGO Authentication* entry, and click *Enable*.

Or

Click the *KERBEROS/SPNEGO Authentication* entry, and then, in the Actions section, click *Enable*.

- 7. In the Actions section, click *Save*.
- 8. When you receive the confirmation message, click *OK*.
- 9. When you receive the message to reload the web application, click *OK*.
- 10. Sign out of your current session.
- 11. Stop and restart the WebFOCUS Reporting Server.
- 12. Sign in as an administrator, and test the configuration.

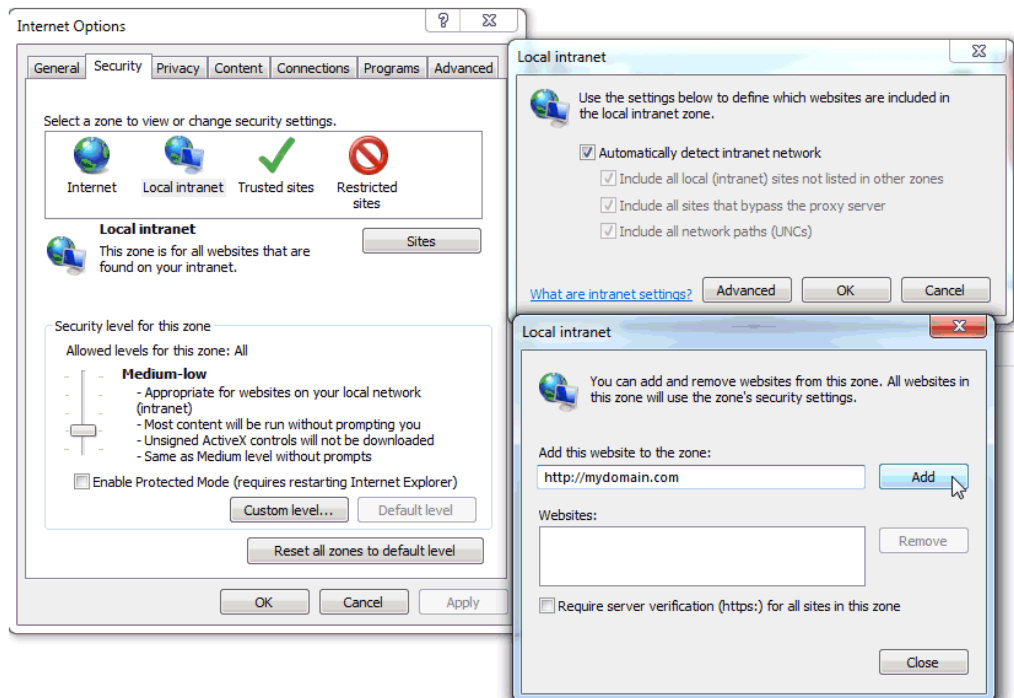
### Web Browser Configuration for Kerberos

The SSO capability requires an Active Directory domain at a Windows 2000 functional level or higher. The following browsers are supported:

- ☐ Microsoft Internet Explorer 10 or higher.
- ☐ Google Chrome™ 53 (although prior versions may also work).
- ☐ Microsoft Edge 44 or higher
- ☐ Mozilla Firefox® 49 or higher (although prior versions may also work).

**Procedure: How to Configure Internet Explorer for Kerberos**

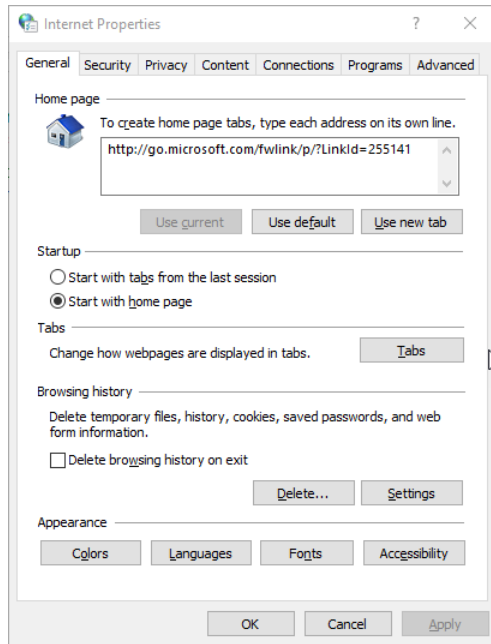
1. Open the Internet Explorer browser menu bar, click *Tools*, and then click *Internet options*.
2. On the Security tab, select the *Local intranet* zone, then click *Sites*.
3. Click *Advanced*.
4. Type either a wildcard for all host names in your DNS that will be considered part of the local intranet, or type the name of just one machine where WebFOCUS runs and click *Add*, as shown in the following image.



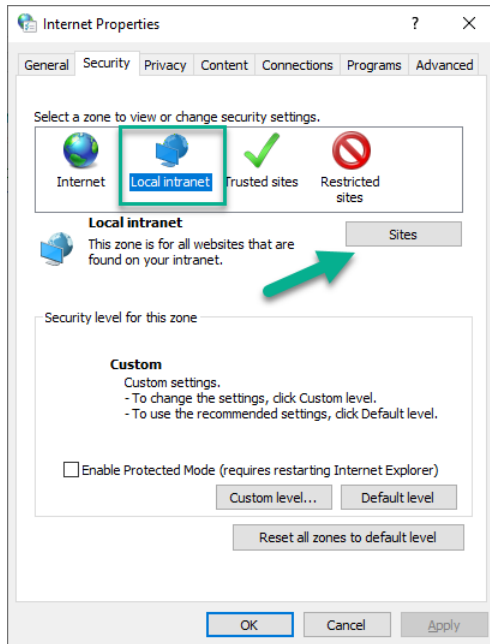
5. Click *Close*, and then click *OK*. In the Internet Options dialog box, click *OK* again to save the change.
6. Open the Internet Options dialog box again, and click the *Advanced* tab. Scroll down to the Security section, and make sure that the *Enable Integrated Windows Authentication* check box is selected.

**Procedure: How to Configure Microsoft Edge for Kerberos**

1. Open the Windows Start menu, and enter *Internet Options* to open the Internet Properties dialog box, as shown in the following image.

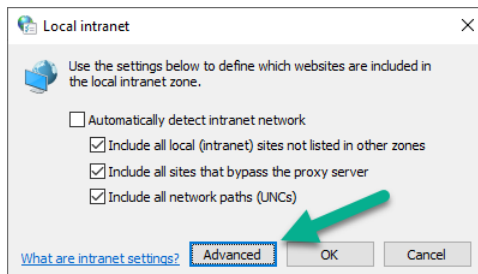


2. Select the *Security* tab, and then select *Local intranet* and *Sites*, as shown in the following image.



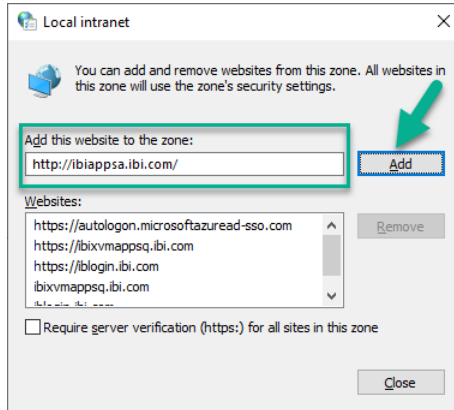
The Local intranet dialog box opens.

3. Select *Advanced*, as shown in the following image.



A second Local intranet dialog box that contains advanced settings opens.

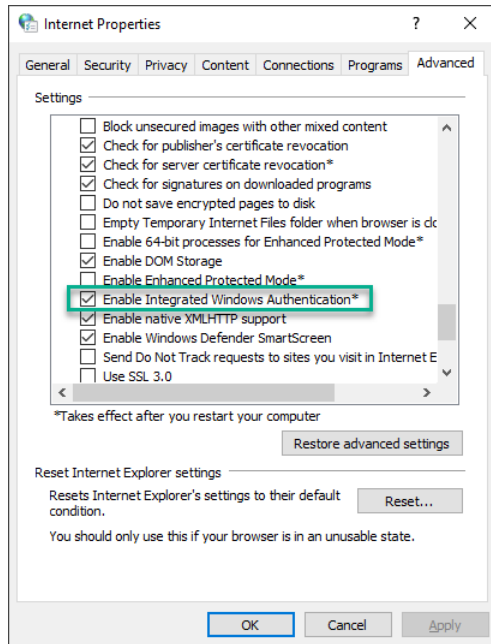
4. Enter a wildcard for all host names in your DNS that will be considered part of the local intranet, or enter the name of just one machine where WebFOCUS runs in the *Add this website to the zone* field, and click *Add*, as shown in the following image.



Repeat this step for each website you must add to the list.

5. When your list of permitted websites is complete, click *Close* to close the Local intranet options dialog box that contains advanced settings, and then click *OK* to close the first Local intranet options dialog box.
6. In the Internet Properties dialog box, select *OK* to close it and save the changes.
7. Open the Internet Properties dialog box again, and select the *Advanced* tab.

8. Scroll down to the Security section, and ensure that the *Enable Integrated Windows Authentication* check box is selected, as shown in the following image.

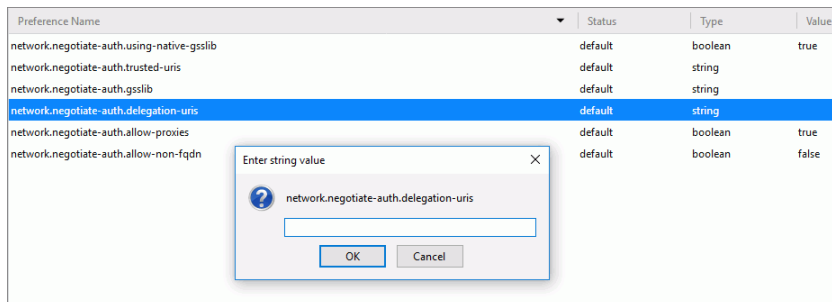


9. When you can confirm that this check box is selected, select *OK* to close the Internet Properties dialog box.

### **Procedure:** How to Configure Mozilla Firefox for Kerberos

1. In the Mozilla Firefox address bar, type *about:config* and press Enter.
2. If you receive a message warning you that this might void your warranty, click *I accept the risk*.
3. Type *network.negotiate* in the Search box to locate the two trust settings. You will add your domain to these two settings.
4. Double-click the *network.negotiate-auth.delegation-uris* entry, as shown in the following image.





5. Add the domain information, then click **OK**.
6. Double-click the *network.negotiate-auth.trusted-uris* entry, add the domain information for the WebFOCUS Reporting Server, and then click **OK**.

## Configuring Google Chrome for Kerberos

The use of Kerberos authentication with the Google Chrome browser requires an Administrator to download and install a Security Policy Template provided by Google.

For browsers hosted on machines that run on Windows, the Security Policy Template adds the following two settings to the Registry.

- ❑ **AuthServerWhitelist.** Specifies the servers that are whitelisted for integrated authentication. Assign the name and domain of any server you wish to include in the WebFOCUS configuration for integrated authentication to this registry value. For example, *webfocus.ibi.com*. If you include multiple server names, separate them with commas. Wildcard characters (\*) are allowed.
  - ❑ **AuthNegotiateDelegateWhitelist.** Specifies the servers to which Google Chrome may delegate authentication tasks. Assign the name and domain of any server that can support authentication tasks to this registry value. For example, *webfocus.ibi.com*. If you include multiple server names, separate them with commas. Wildcard characters (\*) are allowed.
- If you do not assign data to this value, Chrome responds only to integrated authentication requests from an Intranet server and ignores requests from Internet servers.

The Security Policy Template has a similar impact on browsers hosted on machines that run on Apple macOS or Linux. For more information about downloading the Security Policy Template and deploying it in Apple macOS or Linux, see <https://www.chromium.org/administrators/policy-templates>.

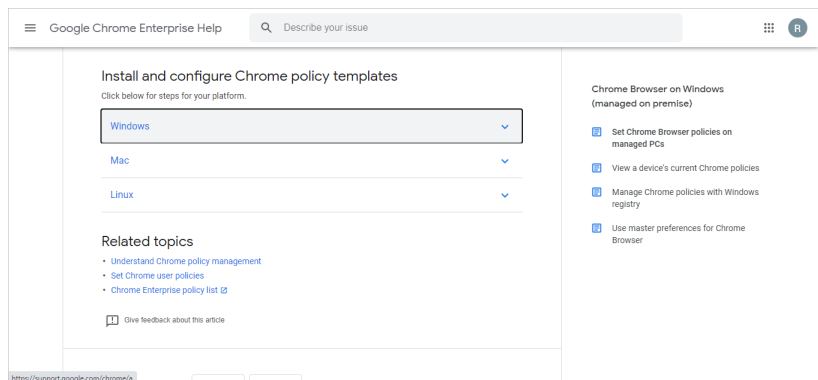
The configuration of Google Chrome browsers to support Kerberos Authentication in Windows is a three-step process:

1. Download the appropriate Security Template, or bundle, from the Google Chrome website.
2. Install the Security Template or policy to the machine that hosts the Google Chrome browser used to access WebFOCUS.
3. Add all the names and URLs of all servers that are made available by Kerberos Authentication to a whitelist maintained in the Windows Registry.

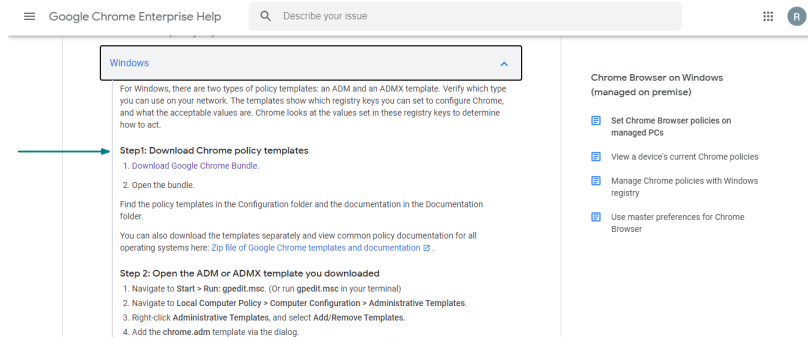
### ***Procedure:*** How to Download the Security Policy Template for Google Chrome Kerberos Authentication

For each user who uses a Google Chrome browser to connect to WebFOCUS:

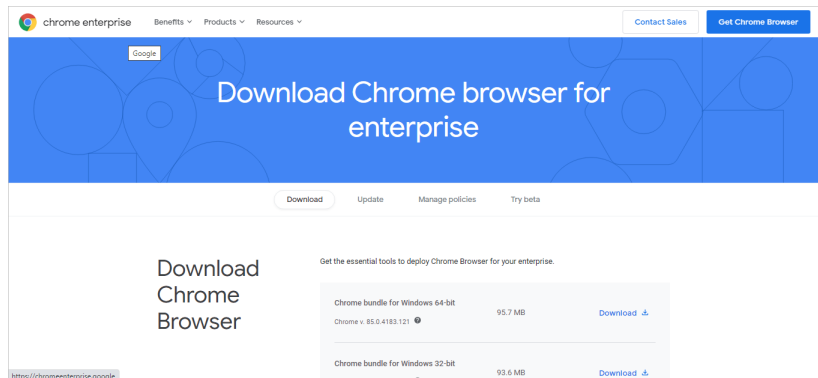
1. Launch the Google Chrome browser and navigate to the *Set Chrome Browser policies on managed PCs Google Chrome Enterprise Help* page, located at the following URL: <https://support.google.com/chrome/a/answer/187202?hl=en>.
2. Scroll down to the *Install and configure Chrome policy templates* section heading, and the subheading that matches the operating system of the device hosting the Google Chrome browser, as shown in the following image.



- Click the Download Google Chrome Bundle link and follow the steps described on the *Get Chrome Browser for Enterprise* page to download the Chrome bundle, as described in step 1 under the Windows subheading and shown in the following image.



- Select the download link next to the Google Chrome Bundle that supports your operating system, as shown in the following image, and follow the prompts from your browser to complete the download.



### **Procedure:** How to Install the Security Policy Templates for Google Chrome Kerberos Authentication in Windows

- Save the Chrome bundle zip file downloaded from the Google Chrome Support site to the local computer, and extract the files stored in it.
- Navigate through the extracted files to:

`drive:\path\Configuration\adm\language\chrome.adm`

where:

`drive:\path\`

Is the drive letter and path to the location where you extracted the zip files.

### *language*

Is the code name for the language used by the machine hosting the Google Chrome browser.

For example:

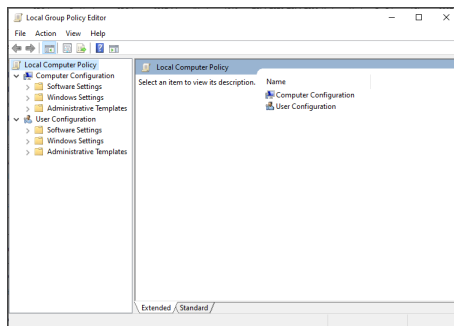
`C:\temp\KerberosUpdatesForEdgeandChrome8207\Configuration\adm\en-US`

3. Open the Local Group Policy Editor by performing one of the following steps.

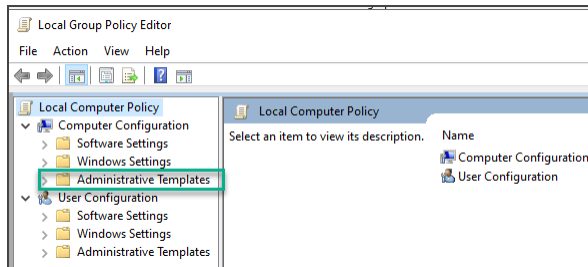
Enter *Edit Group Policy* in the Search Tray of the machine that hosts the browser to open the App panel, and then select *Open* to see the Local Group Policy Editor.

Or

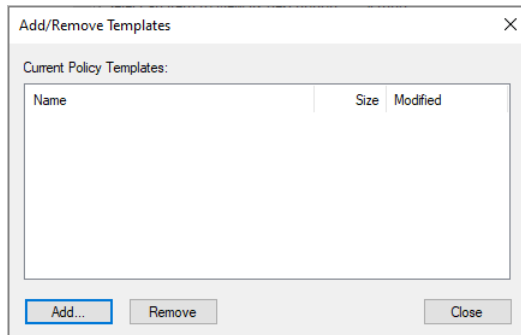
Select *Start* and *Settings*, and then enter *gpedit.msc* in the *Find a Setting* field. Under the Search Results heading, select *Edit Group Policy*, and close the Settings window to see the Local Group Policy Editor, as shown in the following image.



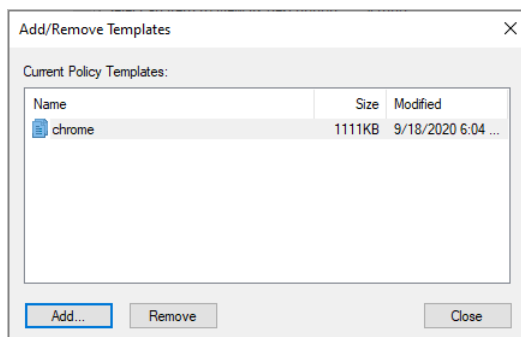
4. In the Local Group Policy Editor, expand *Local Computer Policy*, *Computer Configuration*, and *Administrative Templates* as shown in the following image.



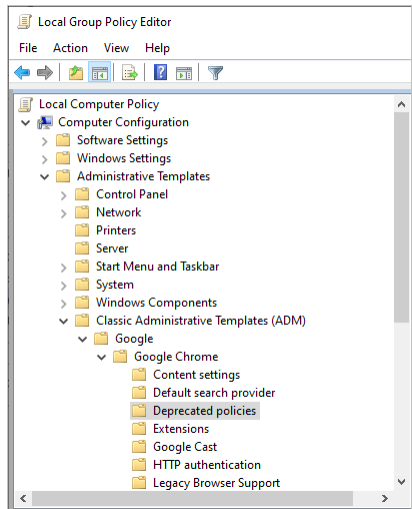
5. Right-click *Administrative Templates*, and select *Add/Remove Templates* from the shortcut menu to open the Add/Remove Templates dialog box, as shown in the following image.



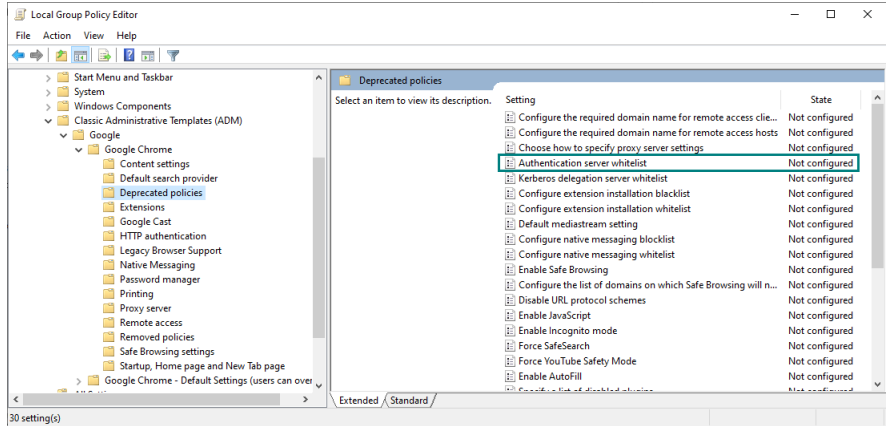
6. Select *Add* and navigate to the network location where you saved the chrome.adm file.
7. Highlight the file and select *Close* to close the Add/Remove Templates dialog box and add the Classic Administrative Templates (ADM) folder to the Local Group Policy Editor, as shown in the following image.



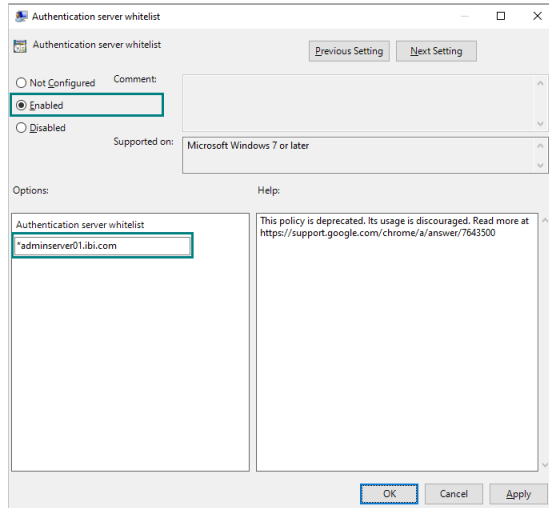
8. Under the Computer Configuration node in the Local Group Policy Editor navigation tree, expand *Administrative Templates*, *Classic Administrative Templates (ADM)*, *Google*, *Google Chrome*, and *Deprecated policies*, as shown in the following image.



9. In the *Deprecated policies* folder, double-click the *Authentication server whitelist* setting, as shown in the following image.



10. In the Authentication server whitelist setting dialog box, select *Enabled*, and in the Options section, enter the name of the server that is whitelisted for integrated authentication, as shown in the following image.



The server name typically takes the format, *server.domain.com*.

where:

*server*

Is the name of the server to be whitelisted for integrated authentication in the WebFOCUS configuration.

*domain*

Is the name of the domain to be whitelisted for integrated authentication in the WebFOCUS configuration.

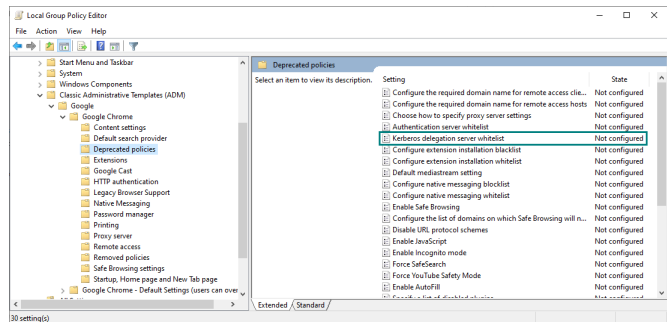
For example:

*adminserver.ibi.com*

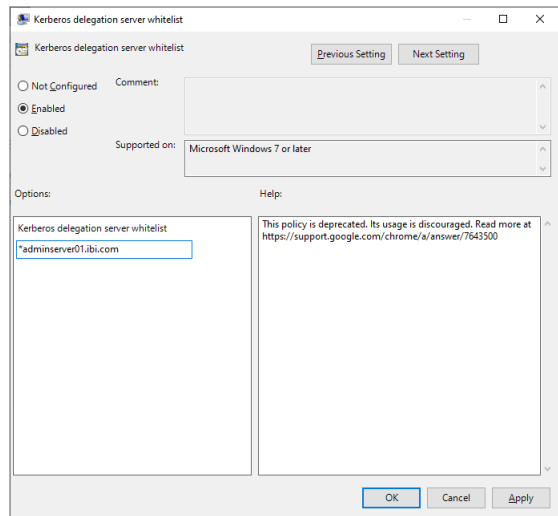
The server name format accepts wildcards. If you need to enter multiple server names, separate each one with a comma (,).

11. Select *OK* to save your changes and close the dialog box.

12. In the *Deprecated policies* folder, select the *Kerberos delegation server whitelist* setting, as shown in the following image.



13. In the *Kerberos delegation server whitelist* dialog box, select *Enabled*, and under the Options section enter the name of the server to allow (accepts wildcards), as shown in the following image.



The server name typically takes the format, *server.domain.com*.

where:

*server*

Is the name of the whitelisted server to which Google Chrome may delegate authentication tasks.

*domain*

Is the name of the whitelisted domain to which Google Chrome may delegate authentication tasks.

For example:



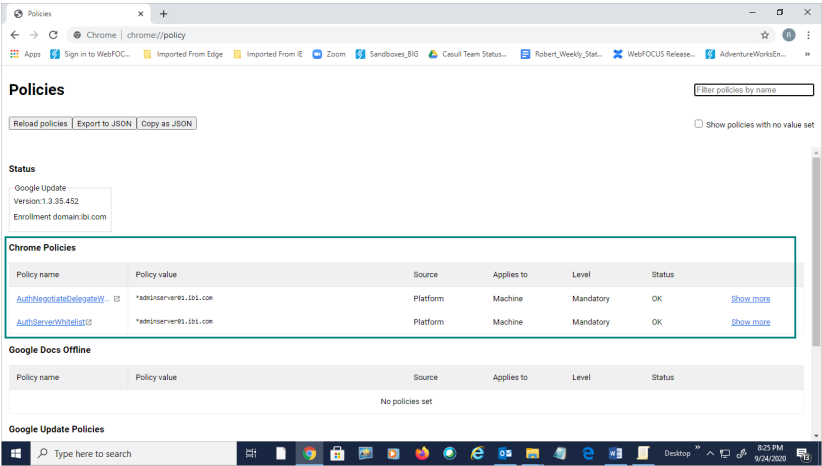
adminserver.ibi.com

The server name format accepts wildcards. IF you need to enter multiple server names, separate each one with a comma (,).

- 14. Click *OK* to save your changes and close the dialog box.
- 15. Select *File* and *Exit* to close the Local Policy Editor.
- 16. Restart the machine that hosts the user’s browser.

**Procedure: How to Confirm That the Google Chrome Browser Accommodates Kerberos Authentication**

- 1. Open the Chrome browser and enter *chrome://policy* in the address bar to open the policy page.
- 2. Review the listings to confirm that the Authentication Server Whitelist policy and the Kerberos Delegation Server Whitelist policy have been implemented, as shown in the following image.



- 3. Confirm that the Policy Value column lists all URLs that are to be made accessible to Kerberos authentication for both policy entries.
- 4. If both policies are present and list the complete set of URLs made accessible by Kerberos authentication, close the browser.
- 5. If one or both policies are missing or if one or more URL is missing, close the browser and edit or reinstall the policy as described in previous topics.

**Procedure: How to Test the WebFOCUS Configuration for Kerberos**

1. Test your Kerberos single sign on configuration by accessing the Business Intelligence Portal (BIP) through one of your previously configured browsers.

The syntax is:

`http://server.url.domain:port/context`

If Kerberos is configured correctly and your user ID has been added to Managed Reporting as previously indicated, you should be signed in to BIP using your Kerberos credentials.

2. Make sure that the WebFOCUS Client can delegate authentication to the WebFOCUS Reporting Server by attempting to run a report against the Kerberos-configured node.

The WebFOCUS Reporting Server edaprint log file will record *request by cmrpip0000xx for Kerberos connect to agent* and reflect your Windows sign-in ID in UPN format.

**Configuring Support for ReportCaster for Kerberos**

Kerberos authentication requires a synchronous connection between the WebFOCUS Reporting Server and the user browser session, but ReportCaster does not use a browser session while running scheduled reports. Therefore, ReportCaster must provide Kerberos with a user ID and password to enable reports.

In the ReportCaster Server Configuration tool, configure each of the data servers that ReportCaster is set up to communicate with. Set the Run Id Type to *User* to ensure that end users are prompted for their user IDs and passwords once for each node.

Alternately, set the Run Id Type to *Static* and provide the user ID and password that will be used for all schedules for that WebFOCUS Reporting Server.

**Procedure: How to Configure the ReportCaster Data Servers for Kerberos**

1. In the ReportCaster Console, click the *Configuration* tab and open the *Data Servers* folder.
2. Select the desired node and change the following settings.
  - a. From the Security Type drop-down list, select *User* or *Static*.
  - b. If you select *Static*, click the button to the right of the User box.
  - c. In the User dialog box, type the user ID and password and click *OK*.
  - d. Click the *Save* button to save your changes.

## Configuring Support for Large Tickets for Kerberos

The Microsoft Windows implementation of Kerberos puts all the Windows group identifiers inside the Kerberos ticket of each user, which can result in a large ticket for a user who belongs to many groups. The Kerberos ticket is transported in an HTTP header, which leads to several technical issues when the ticket size becomes large. If any users belong to more than 100 groups, you may need to perform some or all of the following special configuration tasks:

- ❑ Expand your Tomcat Server HTTP header buffer size. Do this by adding the setting `maxHttpHeaderSize="xx"`, where `xx` is the number of bytes in multiples of 4096. This setting may need to be as high as 65,536 bytes. Add this setting to the 8080 or 8009 connector block in the `server.xml` file for Tomcat, depending on which block you are using.
- ❑ On each workstation accessed by users who belong to many groups:
  - ❑ Configure Windows to use TCP for Kerberos authentication (instead of UDP). This is done in the registry by setting `MaxPacketSize` to 1. For more information, see the *Microsoft Knowledge Base Article 244474* <https://support.microsoft.com/en-us/help/244474/how-to-force-kerberos-to-use-tcp-instead-of-udp-in-windows>.
  - ❑ Configure `MaxTokenSize` to 65535.
- ❑ You must also set `MaxTokenSize` for the domain controllers.

## Setting Up TIBCO WebFOCUS With Kerberos in a Multi-Domain Environment

This topic describes the additional steps that are required for Kerberos to work properly in a multi-domain or subdomain environment.

For example, if you have users who are members of `SUBA.MYDOMAIN.COM`, `SUBB.MYDOMAIN.COM`, and `MYDOMAIN.COM`, and all of those users need to access the Kerberos environment, you must follow the directions in this topic.

To handle the additional configuration settings required for Kerberos to work properly in a multi-domain environment, you must create a Kerberos configuration file named `krb5.ini`. This file contains all the additional information needed for Kerberos to work when you are using more than one domain.

Several versions of Java have a bug that does not allow multiple domains to function properly even with the `krb5.ini` configuration. As a result, you may need to update your version of Java. For details on the Java bug, go to the following Java bug report:

[http://bugs.sun.com/view\\_bug.do?bug\\_id=6670362](http://bugs.sun.com/view_bug.do?bug_id=6670362)

**Procedure: How to Create a krb5.ini File to Handle Kerberos Settings**

1. Create a new text file named *krb5.ini*.

You can create this file anywhere on the file system, since you explicitly refer to its location later. For the purpose of this example, create the file in:

```
drive:\ibi\WebFOCUS82\config\krb5.ini
```

2. At the beginning of the *krb5.ini* file, insert the following lines of code for the [libdefaults] section.

Replace the default\_realm name, MYDOMAIN.COM, in the last line of the example with the fully qualified DNS name for the domain of the machine that the WebFOCUS Client has joined.

Type the default\_realm name in uppercase letters, as it is case-sensitive.

```
[libdefaults]
    ticket_lifetime = 600
    default_tgt_enctypes = rc4-hmac
    default_tgs_enctypes = rc4-hmac
    default_checksum = rsa-md5
    forwardable = true
    default_realm = MYDOMAIN.COM
```

3. After the [libdefaults] section, insert the following lines of code for the [realms] section. Include an entry for every domain and subdomain that you will use, as shown in the following example.

If the domains and subdomains share domain controllers, you can create a [realms] section here, and refer to the relationships in the next section, [domain\_realm]. The [domain\_realm] section is described in step 4.

```
[realms]
MYDOMAIN.COM = {
    kdc = dc1.mydomain.com:88
    kdc = dc2.mydomain.com:88
    kdc = dc3.mydomain.com:88
    default_domain = mydomain.com
}
SUBA.MYDOMAIN.COM = {
    kdc = dc1.suba.mydomain.com:88
    kdc = dc2.suba.mydomain.com:88
    default_domain = suba.ibi.com
}
SUBB.MYDOMAIN.COM = {
    kdc = dc1.subb.mydomain.com:88
    kdc = dc2.subb.mydomain.com:88
    default_domain = subb.ibi.com
}
```

As in the [libdefaults] section, the values in the [realms] section are case-sensitive. For instance, the first reference name (such as MYDOMAIN.COM in the first block in the example) must be uppercase and the value for default\_domain must be lowercase.

Each entry for kdc must refer to the DNS name of a domain controller for the applicable domain. Only one kdc entry is required per domain listed, but multiple kdc entries allow for redundancy.

4. This step is optional. To map additional domains or host names to a specific realm, insert the following lines of code in the optional [domain\_realm] section.

A domain maps to the realm of the same name, but the realm name is uppercase. As a result, the following entries are redundant:

```
[domain_realm]
.suba.mydomain.com = SUBA.MYDOMAIN.COM
.subb.mydomain.com = SUBB.MYDOMAIN.COM
.mydomain.com = MYDOMAIN.COM
```

For more information on the [domain\_realm] section, see the MIT Kerberos specifications at the following website:

[http://web.mit.edu/kerberos/krb5-1.4/krb5-1.4.1/doc/krb5-admin/domain\\_realm.html](http://web.mit.edu/kerberos/krb5-1.4/krb5-1.4.1/doc/krb5-admin/domain_realm.html)

5. This step is optional. If applicable at your site, insert the following lines of code in the optional [capaths] section.

The [capaths] section is needed only in environments in which the parent domain does not have unilateral trust relationships with all the child domains, or in environments in which multiple domain hierarchies are used.

In those situations, the Kerberos protocol is not able to determine how to authenticate a user from one domain, for a resource in another domain. As a result, the relationships required to accomplish the authentication need to be mapped so that Kerberos knows which path to take to authenticate a user. The following trust relationships apply:

- ☐ Domain SUBA.MYDOMAIN.COM unilaterally trusts SUBB.MYDOMAIN.COM.
- ☐ Domain SUBB.MYDOMAIN.COM unilaterally trusts MYDOMAIN.COM.
- ☐ Domain SUBA.MYDOMAIN.COM does not trust MYDOMAIN.COM.

In this example, Kerberos can directly authenticate any user from SUBA.MYDOMAIN.COM, for any resource in SUBB.MYDOMAIN.COM. To authenticate a user in SUBA.MYDOMAIN.COM with MYDOMAIN.COM, you must authenticate that user through SUBB.MYDOMAIN.COM, since SUBA.MYDOMAIN.COM does not have a direct trust relationship with MYDOMAIN.COM.

```
[capaths]
SUBA.MYDOMAIN.COM {
SUBB.MYDOMAIN.COM = .
MYDOMAIN.COM = SUBB.MYDOMAIN.COM
}
SUBB.MYDOMAIN.COM {
SUBA.MYDOMAIN.COM = .
MYDOMAIN.COM = .
}
MYDOMAIN.COM {
SUBB.MYDOMAIN.COM = .
SUBA.MYDOMAIN.COM = SUBB.MYDOMAIN.COM
}
```

In the first block is the information for authenticating a user from SUBA.MYDOMAIN.COM. Kerberos can directly authenticate a user from SUBA.MYDOMAIN.COM against SUBB.MYDOMAIN.COM, as represented by the period (.). To authenticate a user from SUBA.MYDOMAIN.COM against MYDOMAIN.COM, Kerberos must go against SUBB.MYDOMAIN.COM. That is why the code states MYDOMAIN.COM =SUBB.MYDOMAIN.COM.

In the second block is the information for authenticating a user from SUBB.MYDOMAIN.COM. Since Kerberos can directly authenticate a user from SUBB.MYDOMAIN.COM against both SUBA.MYDOMAIN.COM and MYDOMAIN.COM, a period (.) is included in both of those columns.

In the third block is the information for authenticating a user from MYDOMAIN.COM. Kerberos can directly authenticate a user from MYDOMAIN.COM, for resources in SUBB.MYDOMAIN.COM, as represented by a period (.). Kerberos must authenticate a user from SUBA.MYDOMAIN.COM by first going through SUBB.MYDOMAIN.COM.

For more information on the use of the [capaths] section with the Kerberos protocol, see the following document from MIT:

<http://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-admin/capaths.html>

Your krb5.ini file will look similar to the following when you are done:

```

[libdefaults]
    ticket_lifetime = 600
    default_tgt_enctypes = rc4-hmac
    default_tgs_enctypes = rc4-hmac
    default_checksum = rsa-md5
    forwardable = true
    default_realm = MYDOMAIN.COM
[realms]
MYDOMAIN.COM = {
    kdc = dc1.mydomain.com:88
    kdc = dc2.mydomain.com:88
    kdc = dc3.mydomain.com:88
    default_domain = mydomain.com
}
SUBA.MYDOMAIN.COM = {
    kdc = dc1.suba.mydomain.com:88
    kdc = dc2.suba.mydomain.com:88
    default_domain = suba.ibi.com
}
SUBB.MYDOMAIN.COM = {
    kdc = dc1.subb.mydomain.com:88
    kdc = dc2.subb.mydomain.com:88
    default_domain = subb.ibi.com
}
[domain_realm]
    .suba.mydomain.com = SUBA.MYDOMAIN.COM
    .subb.mydomain.com = SUBB.MYDOMAIN.COM
    .mydomain.com = MYDOMAIN.COM

[capaths]
SUBA.MYDOMAIN.COM {
SUBB.MYDOMAIN.COM = .
MYDOMAIN.COM = SUBB.MYDOMAIN.COM
}
SUBB.MYDOMAIN.COM {
SUBA.MYDOMAIN.COM = .
MYDOMAIN.COM = .
}
MYDOMAIN.COM {
SUBB.MYDOMAIN.COM = .
SUBA.MYDOMAIN.COM = SUBB.MYDOMAIN.COM
}

```

### **Procedure:** How to Specify the Location of krb5.ini in Apache Tomcat

For WebFOCUS Kerberos configurations, the krb5.ini is typically required. You must refer to the location of the file using the following Java™ option. You can specify the -Djava.security.krb5.conf option in Tomcat, as described in the following procedure.

1. Navigate to the bin directory of Tomcat.

Typically, the bin directory is in the following location:

`drive:\ibi\tomcat\bin\`

2. Double-click `tomcat8Wfw.exe` to open the Tomcat configuration dialog box.
3. Select the *Java* tab and add the following entry to the end of the list of Java Options.

`-Djava.security.krb5.conf=drive:\ibi\WebFOCUS82\config\krb5.ini`

If you chose another location in which to store your `krb5.ini` file, you must refer to that location, instead of the location in the preceding example.

4. Click *Apply* to save the setting.
5. Stop Tomcat and then restart it for the setting to take effect.

## Configuring Pre-Authentication with SAML

Security Assertion Markup Language (SAML) authentication relies on the use of a third-party identity provider to assert the authentication of a user requesting services from a service provider. When a principal, such as a WebFOCUS user, requests services from a service provider, such as WebFOCUS, the service provider relays the request to the identity provider, who then authenticates the principal and allows the requests. SAML pre-authentication allows administrators to transfer the burden of user account maintenance to an independent provider dedicated to this task, and frees users from having to sign in multiple times during a work session, in order to open WebFOCUS and other applications. WebFOCUS supports a variety of identity providers with varying requirements for internal security and credential-based authentication. You can obtain additional information about any specialized support requirements for them by contacting Customer Support.

The complete configuration for SAML Authentication includes the following activities:

1. Create a customized keystore.

**Note:** This step is optional but recommended.

You can use the default keystore delivered with WebFOCUS to support SAML authentication, or you can create a customized keystore. You can limit the keystore to SAML authentication support, or you can use it to support other security features that require the use of a keystore, such as trusted ticket authentication. If you create a customized keystore, you need to add it to the Key Management dialog box, and add the values you assign to it to the SAML Service Provider metadata defined in the Edit SAML Authentication dialog box



## 2. Enable the Alternate Security Zone

After establishing SAML authentication in the Default Security Zone, administrators will still need to bypass SAML authentication for configuration and maintenance activities. By enabling the Alternate Security Zone, which is configured to use form-based authentication by default, administrators can continue to sign in from their machines, and authenticate themselves appropriately while bypassing SAML authentication.

## 3. Assign the customized keystore to WebFOCUS.

**Note:** This step is optional but recommended.

If you create a customized keystore, you must make it available to WebFOCUS by adding it to the Certificate Alias and Password Map in the Key Management dialog box, and replacing the location and password of the default keystore with those of the customized keystore. However, you can skip this activity if you use the default keystore. It is already configured within this dialog box.

## 4. Download and configure the SAML service provider metadata file

Add the keystore certificate alias and password to the SAML Service Provider metadata in the Edit SAML Authentication dialog box. Use these values, along with the Entity ID and Entity Base URL, to generate a metadata file that identifies WebFOCUS as a trusted service provider to the identity provider that supports SAML authentication.

## 5. Download and configure the identity provider metadata file to WebFOCUS

Add the metadata file provided by the identity provider to the WebFOCUS configuration in order to enable it to use that provider to authenticate user identities.

## 6. Enable SAML authentication in the Default Security Zone

To establish SAML authentication as the default method of authentication for WebFOCUS users, you must disable all other forms of authentication in the Default Security Zone and enable SAML authentication.

## 7. Save the SAML authentication configuration

Save the settings configured in the Edit SAML Authentication Settings dialog box by clicking the Save link on the Authentication Page. Sign out and recycle the WebFOCUS Reporting Server to complete the implementation of SAML authentication.

Even when you establish SAML Authentication as the principal method of authentication for the production environment, we recommend that you retain the use of form-based authentication by enabling the Alternate Security Zone and leaving it configured to use form-based authentication. You can continue to use the Alternate Security Zone for system maintenance tasks under a form based sign in.

### Notes:

- ❑ In keeping with the OASIS Standard, WebFOCUS rejects SAML Authentication Request <AuthnRequest> messages initiated from identity providers that do not contain the <SubjectConfirmationData> element with the HTTP 401 Unauthorized error stating that the request has not been applied because it lacks valid authentication credentials for the target resource. For more information about the OASIS Standard for <AuthnRequest> messages, see <https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>, pages 18 and 19.
- ❑ In keeping with the Spring Security SAML Extension standard, WebFOCUS processes and validates authenticated sign-in requests initiated by identity providers, also known as Unsolicited Response messages or IDP-initialized SSO messages, in exactly the same way as authentication requests initiated by service providers. It evaluates the authentication provided with the request and grants access to the principal or returns an error based on the validation of the identity of the requestor by the identity provider. For more information about the Spring Security SAML Extension standard for <AuthnRequest> messages, see <http://docs.spring.io/spring-security-saml/docs/1.0.2.release/reference/pdf/spring-security-saml-reference.pdf>, page 32.

### SAML Authentication Prerequisites

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

There may be additional prerequisites, such as configuring WebFOCUS for SSL. For an introduction to the steps required by the SSL configuration, see [Configuring TIBCO WebFOCUS for SSL](#) on page 51. For information about other prerequisites, contact Customer Support.

We recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

### **Procedure:** How to Create a Customized Keystore

This procedure is optional. You can use the default keystore, wfKeystore.jks, and the default alias within it to support SAML Authentication operations.

- ❑ To use the default keystore and alias, skip this procedure. Use the default settings in the Key Management dialog box and the Edit SAML Authentication Settings dialog box.

- ❑ To use a customized keystore and alias, follow this procedure. You must also add settings for the new keystore to the Key Management dialog box and replace the default settings in the Edit SAML Authentication Settings dialog box with those you use to create the customized keystore.

1. Open the command prompt window and redirect the command prompt to the *drive:\ibi\WebFOCUS82\config\was* directory.
2. Type the Java keytool command and values as shown in the following example:

```
keytool -genkey -alias aliasname -keyalg RSA -keysize 2048 -keypass keypass
-keypass storepass -storepass storepass -validity 3650 -keystore keystorename.jks
```

where:

*aliasname*

Is the unique alias assigned to the private key contained within the keystore.

*RSA*

Is the algorithm assigned to the keystore.

*2048*

Is the keysize.

*keypass*

Is the password assigned to the private key alias.

*storepass*

Is the password assigned to the keystore file.

*3650*

Is the number of days the key is valid.

*keystorename.jks*

Is the name assigned to keystore file.

**Note:** keytool is a Java command typically found in the Java bin directory.

3. Press the Enter key.

The command prompt displays the first in a series of questions.

4. Respond to each question as follows:

- ❑ "What is your first and last name?" Type the first and last name of the certificate holder.

For example, *John Doe*

- ❑ "What is the name of your organizational unit?" Type the name of the organizational unit of the certificate holder.

For example, *Technical Content Management*

- ❑ "What is the name of your organization?" Type the name of the organization of the certificate holder.

For example, *TIBCO*

- ❑ "What is the name of your City or Locality?" Type the name of the city or locality of the certificate holder.

For example, *New York*

- ❑ "What is the name of your State or Province?" Type the two-letter abbreviation for the state in which the certificate holder is located.

For example, *NY*

- ❑ "What is the two-letter country code for this unit?" Type the two-letter abbreviation for the country in which the certificate holder is located.

For example, *US*

5. When the command prompt displays the question, "Is CN=\_\_, OU=\_\_, O=\_\_, L=\_\_, ST=\_\_, C=\_\_ correct?" review the values and type *y* if they are correct.

For example, Is CN= John Doe, OU= Technical Content Management, O= TIBCO, L= New York, ST= NY, C= US correct?

If they are not correct, type *n* and retype the keytool command from step 2.

If they are correct, the new keystore is ready for use.

6. Type the keytool command again to review and confirm the details of the new keystore, as shown in the following example:

```
keytool -list -v -keystore keystorename.jks -storepass storepass
```

where:

*keystorename.jks*

Is the name assigned to the keystore file.

*storepass*

Is the password assigned to the keystore file.

7. Ensure that the new keystore file is saved to the following directory:

```
drive:\ibi\WebFOCUS82\config\was
```

**Procedure: How to Assign a Customized Keystore to TIBCO WebFOCUS**

You can use the default keystore, wfKeystore.jks, and the default alias to sign and encrypt WebFOCUS certificates for the identity provider. You can substitute a customized keystore and alias if your identity provider requires.

- ☐ To use the default keystore and alias, skip this procedure and use the default settings in the Key Management dialog box.
  - ☐ To use a customized keystore and alias, follow this procedure, and replace the default settings in the Key Management dialog box with those you used to create the customized keystore.
1. In the Administration Console, on the Security tab, under the Security Zones folder, expand the *Default Security Zone* folder, and then click *Authentication*.
  2. On the Authentication page, click *Key Management*.
  3. In the Key Management dialog box, accept the default value in The Location of the Keystore File field.

This location corresponds to the location where you placed the keystore when you created it, *drive:\ibi\WebFOCUS82\config\was*.

4. Type the password you assigned to the keystore in The Password for the Keystore field.  
This is the password you assigned to the storepass option when you created the keystore.
5. Click *Add*.
6. Type the alias you assigned to the keystore in the Certificate Alias in the Keystore field.
7. Type the password you assigned to the keystore alias in the Password field.
8. Select the *Default Certificate Alias* check box.
9. Click *OK*.

The entry for the new keystore appears in The Certificate Alias and Password Map box.

10. Click *OK*.

**Procedure: How to Configure and Generate TIBCO WebFOCUS Metadata for a SAML Authentication Provider**

Before you begin this configuration, ensure that a keystore is available in the following directory:

*drive:\ibi\WebFOCUS82\config\was*

You can use the default keystore, `wfKeystore.jks`, and the default alias to sign and encrypt WebFOCUS certificates for the identity provider, or you can substitute a customized keystore and alias, if your identity provider requires.

- ☐ To use the default keystore and alias, use the default settings in the Edit SAML Authentication Settings dialog box.
- ☐ To use a customized keystore and alias, replace the default settings in the Edit SAML Authentication Settings dialog box with those you used to create the customized keystore.

1. In the Administration Console, on the Security tab, under the Security Zones folder, expand the *Default Security Zone* folder and then click *Authentication*.
2. Double-click the *SAML Authentication* entry.

The Edit SAML Authentication Settings dialog box opens.

3. On the Service Provider (SP) Metadata tab, in the Location of the Metadata File field, accept the default location and file name, or type the path name to an alternate location and file name if you must use one for your installation of WebFOCUS.

The default location is:

`file:{IBI_CONFIGURATION_DIRECTORY}/was/saml/wfspMetadata.xml`

where:

`IBI_CONFIGURATION_DIRECTORY`

Is the value that identifies the path from the root directory to the sub-folders that follow this setting. For example:

`drive:\ibi\WebFOCUS82\config\`

4. In the Entity Alias field, type over the default value with an easily recognizable name, such as the host name, that uses only alphanumeric characters.
5. If you are using the default keystore provided in the product installation, accept the default values in the Signing Certificate Alias field and Encryption Certificate Alias field. Otherwise, type the alias you added to the customized keystore in these fields.

These values identify the WebFOCUS alias as the presenter of the Signing Certificate and the Encryption Certificate to the SAML identity provider.

6. Accept the default values assigned to the SSL/TLS Certificate Alias, Security Profile, and SSL/TLS Security Profile fields.
7. The Sign Metadata check box is cleared, by default. Select this check box only if there is a need to digitally sign WebFOCUS metadata you submit to the Identity Provider.
8. Accept the default settings assigned to the Support Single Logout check box and the Require Signed Logout Request check box.

9. The Require Signed Logout Response check box is cleared, by default. Select this check box only if you need to authenticate responses from the identity provider.
10. Click *Generate Metadata*.

The Service Provider (SP) Metadata Generation dialog box opens.

11. In the Entity ID field, accept the default URL, or type the URL that the Service Provider will use when communicating with the WebFOCUS Client.

**Note:** If the value *localhost* appears in this field, you must replace it with the fully-qualified URL that is used to access WebFOCUS. For example:

[https://SERVER.DOMAIN.COM/ibi\\_apps/sp](https://SERVER.DOMAIN.COM/ibi_apps/sp)

12. In the Entity Base URL field, accept the default URL, or type the base of the URL that the Service Provider will use when communicating with the WebFOCUS Client.

**Note:** If you are configuring SAML Authentication for the Alternate Security Zone, and the value *localhost* appears in this field, you must replace it with a fully-qualified URL that is used to access WebFOCUS. For example:

[https://SERVER.DOMAIN.COM/ibi\\_apps](https://SERVER.DOMAIN.COM/ibi_apps)

13. Bypass the remaining unavailable settings. If you need to update or change the values assigned to them, close the Service Provider (SP) Metadata Generation dialog box and update the corresponding fields in the Edit SAML Authentication Settings dialog box.
14. Accept the default selection of The Service Signs Authentication Requests check box and the Require Signed Authentication Assertion check box.
15. Accept the default selections in the Single Sign-on Bindings section and in the Supported Name IDs section.
16. Click *Generate*.
17. Follow the directions in your browser to download the wfspMetadata.xml file to your desktop.

18. Copy the wfspMetadata.xml file from your desktop to the following directory on the WebFOCUS machine:

[drive:\ibi\WebFOCUS82\config\was\saml](#)

19. Click *Cancel* to close the Service Provider (SP) Metadata Generation dialog box.
20. Transfer the wfspMetadata.xml file to your identity provider for use in establishing a trusted relationship with your WebFOCUS environment.
21. Continue with the addition of the identification service provider metadata file to the Edit SAML Authentication Settings dialog box.

In the rare event that no metadata file is available from the identification service provider, click *OK* to close the Edit SAML Authentication Settings dialog box and save the Authentication page, as described in, [How to Save a SAML Configuration](#) on page 310.

**Procedure: How to Download and Configure the Identity Provider Metadata File to the SAML Configuration**

Before you begin this configuration, ensure that the SAML Identity provider has delivered a metadata file to you.

1. Download the metadata file delivered to you from the SAML identity provider.
2. Copy the metadata file from the identity provider to the following location:  
`drive:\ibi\WebFOCUS82\config\was\saml`
3. Open the Edit SAML Authentication Settings dialog box, and click the *Identity Provider (IDP) Metadata* tab.
4. On the Identity Provider (IDP) Metadata tab, in the Location of the Metadata File field, type the name of the metadata file from the identity provider.

Use the following format:

```
file:{ IBI_CONFIGURATION_DIRECTORY }/was/saml/idpMetadata.xml
```

where:

`IBI_CONFIGURATION_DIRECTORY`

Is the value that identifies the path from the root directory to the sub-folders that follow this setting, for example:

```
drive:\ibi\WebFOCUS82\config\
```

5. Accept the default value for all of the remaining settings on the Identity Provider (IDP) Metadata tab.

Change these settings only if required by your identity provider.

6. Click the *Advanced* tab.

**Note:** Settings on the Advanced tab are configured automatically when you generate a metafile. Typically, there is no need to adjust these settings. However, you can clear or select the following check boxes, if required.

- a. By default, the *Retrieve User Name from SAML Assertion Attribute* check box is cleared. If your authentication provider supports this feature, you can activate it by selecting this check box and entering the name of the SAML assertion attribute that contains the user name.



The user name retrieved from this attribute can be used to support external authorization. For more information, see [Understanding External Authorization](#) on page 326.

- b. By default, the *Retrieve User Groups from SAML Assertion Attribute* check box is cleared. If your authentication provider supports this feature, you can activate it by selecting this check box and accepting the *member-of* default value or entering the name of the SAML assertion attribute that contains the user group name.

The group name retrieved from this attribute can be used to support external authorization. For more information, see [Group Mapping](#) on page 333.

- c. By default, the *Use SHA256withRSA for Signature Algorithm* and *SHA-256 for Digest Algorithm* check box is cleared. Select this check box if your identity provider either supports the SHA256 hash algorithm, or is configured to use it for the relying party trust.
  - d. By default, the *Disable Service Provider Initialized Single Sign-On* check box is cleared. Select this check box only if you must block single sign-on authentication requests initiated by WebFOCUS, the service provider.
  - e. By default, the *Redirect to RelayState URL after Successful Sign-On* check box is cleared. Select this check box if users are to be redirected automatically to a valid URL identified by their identity provider after a successful sign-in.
7. Click *OK* to close the Edit SAML Authentication Settings dialog box, and save your changes.

### **Procedure: How to Enable SAML Authentication in the Default Zone**

When SAML Authentication is enabled in a security zone, all other methods of authentication in that zone must be disabled.

1. In the Administration Console, on the Security tab, under the Security Zones folder, expand the Default Security Zone folder, and then click *Authentication*.
2. On the Authentication page:
  - a. Click the *Form Based Authentication* entry, and then click *Disable*.
  - b. Click the *Anonymous Authentication* entry, and then click *Disable*.
  - c. Click the *SAML Authentication* entry, and then click *Enable*.
3. Save the Authentication page with the SAML Configuration as described in, [How to Save a SAML Configuration](#) on page 310.

**Procedure: How to Enable the Alternate Security Zone**

Enabling the Alternate Security Zone makes form based authentication accessible to administrators when they must bypass SAML authentication for configuration and administration tasks.

1. In the Administration Console, on the Security tab, click the *Security Zones* folder.
2. On the Security Zones page, click the *Alternate Security Zone* entry, and then, in the Actions section, click *Enable*.

The status changes from Disabled to Enabled, and the Alternate Security Zone is ready for use.

**Procedure: How to Save a SAML Configuration**

1. In the Actions section of the Authentication page, click Save.
2. When you receive a confirmation message, click *OK*.
3. When you receive a message to reload the web application, click *OK*.
4. Sign out of your current session.
5. Stop and restart the WebFOCUS Reporting Server.
6. Sign in as an administrator, and test the new configuration.

**Configuring Trusted Ticket Authentication for Embedded BI Applications**

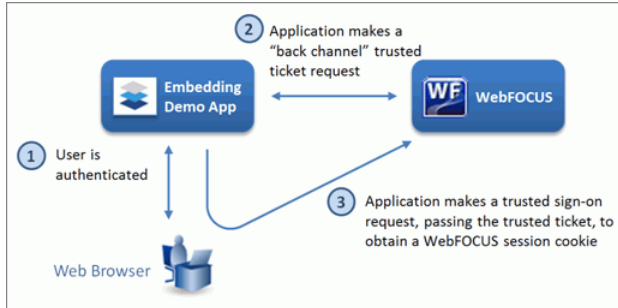
Trusted ticket pre-authentication uses a trusted ticket to authenticate the identity of a user requesting access to WebFOCUS content and resources that are embedded in a trusted Embedded BI (Business Intelligence) Application. WebFOCUS provides this trusted ticket to an Embedded BI Application during the sign-in process.

Trusted ticket authentication makes it possible for users of an Embedded BI Application to take advantage of the single sign on (SSO) capability. It also protects WebFOCUS by ensuring that the resources it provides are only made available to known users who maintain defined roles and access privileges.

To support this method, both the Embedded BI Application and WebFOCUS must maintain records of Embedded BI Application users, and these users must be assigned to groups in the domains that contain the content and resources embedded in the external application. The Embedded BI Application must be configured to send the variables that support trusted ticket authentication, and WebFOCUS must be configured to accept these variables in the Security Zone that supports Embedded BI Applications.

## Tracing the Trusted Ticket Authentication Workflow

Trusted ticket authentication requires three exchanges of messages, as shown in the following image.



### User Sign-In to the Embedded BI Application

In the first exchange, users sign in to an Embedded BI Application. To sign in, users present credentials, such as a User ID and Password, that identify them as valid users with the authority to work within that application. The Embedded BI Application authenticates their credentials, and begins the work session.

### Trusted Ticket Request

In the second exchange, the Embedded BI Application submits an HTTP GET or POST request message for a trusted ticket from WebFOCUS. For example:

```
GET http://host:port/ibi_apps/service/wf_security_trusted.jsp?
IBIB_userid=userone
```

**Note:** You can use `http://` or `https://` for this request.

This second exchange of messages between the Embedded BI Application and WebFOCUS is typically referred to as a *back channel* request because the connection is established directly between the server hosting the Embedded BI Application and the server hosting WebFOCUS. Therefore, the connection is not seen by the network that runs the web browser of the user.

This trusted ticket request includes one required parameter and two optional parameters.

- ❑ The `IBIB_userid` parameter is required. It contains the ID of the newly-authenticated user.
- ❑ The `IBIB_appname` parameter is optional. It contains the name of one of the applications identified in the Application List of the Trusted Ticket Authentication Settings dialog box. It can be included in the trusted ticket request, but if it is not included, and a default application has been identified for the security zone, WebFOCUS uses the default application name specified in the Trusted Ticket Authentication Settings dialog box.

- ❑ The IBIB\_useripaddr parameter is also optional. It is required only if the *Enable Client IP Matching* check box is selected in the Application Settings for Trusted Ticket dialog box for the Embedded BI Application. This parameter contains the IP address of the browser of the user who initiated the sign-on request.

When WebFOCUS receives a trusted ticket request, it determines if the request includes an IBIB\_appname parameter. If the request includes this parameter, WebFOCUS ensures that the application is one of the valid applications on the Application List of the Trusted Ticket Authentication Settings dialog box.

If there is no match for the application name in the IBIB\_appname parameter, the trusted ticket request is rejected.

If there is a match for the application name, WebFOCUS then compares the IP address of the application requesting the trusted ticket to the list of Accepted IP Addresses for that application. If the IP address is not included in that list, the request is rejected. If the IP address is included in that list, the trusted ticket is created.

If the IBIB\_appname parameter is not included in the trusted ticket request, WebFOCUS determines if any of the applications in the list are identified as the default application.

If there is no default application, the request is rejected.

If there is a default application, WebFOCUS determines if the IP Address of the application requesting the trusted ticket is included in the IP Accepted Address list for the default application. If it is not included in the list, the request is rejected. If it is included in the list, a trusted ticket is created.

The trusted ticket contains encrypted information that is utilized by WebFOCUS for the subsequent trusted sign-on request. The trusted ticket takes values from the parameters in the trusted ticket request, including the required IBIB\_userid parameter, the optional IBIB\_appname and IBIB\_useripaddr parameters, and the time at which the ticket was created. Later, in the trusted sign-on request, WebFOCUS uses the encrypted values from these parameters to validate the authenticity of the user and the trusted sign-on request itself. The trusted ticket must be returned to WebFOCUS as part of a trusted sign-on request within the time specified by the ticket validity period for that application. The length of this period is defined in *The ticket validity period (seconds)* field in the Application Settings for Trusted Ticket dialog box for each Embedded BI Application.

When the trusted ticket is created, WebFOCUS returns it to the Embedded BI Application. This application then returns the trusted ticket to the browser of the user who initiated the sign-on request.

### Trusted Sign-on Request

In the third exchange, the browser of the user of the Embedded BI Application submits a trusted sign-on request to WebFOCUS. This request takes the form of an HTTP GET or POST request message to WebFOCUS. For example:

```
GET http://host:port/ibi_apps/service/wf_security_trusted.jsp
```

where:

*host*

Is the name or IP address of the host used to access WebFOCUS.

*port*

Is the number of the port on which the Web Server or Application Server listens.

This value is optional, and it should be excluded if the URL uses the default port for the protocol it uses in the scheme, which is port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

**Note:** You can use *http://* or *https://* for this request.

This trusted ticket sign-on request includes one required parameter and two optional parameters.

- ☐ The IBIB\_ticket parameter is required. It contains the trusted ticket value obtained from the Embedded BI application.
- ☐ The IBIB\_appname parameter is optional. It contains the name of one of the applications identified in the Application List of the Trusted Ticket Authentication Settings dialog box. It can be included in the trusted sign-on request, but if it is not included, and a default application has been identified for the security zone, WebFOCUS uses the default application name specified in the Trusted Ticket Authentication Settings dialog box.
- ☐ The IBIB\_Destination parameter is also optional. It contains the URL to which WebFOCUS will redirect the user after signing in. This destination can be the WebFOCUS Home Page or a portal that is identified by a relative URL.

When WebFOCUS receives a trusted sign-on request, it ensures that the request arrived within the ticket validity time period defined for the Embedded BI Application of the user that initiated the trusted sign-on request, and that the user making the request exists within WebFOCUS. If the trusted sign-on request occurs after the ticket validity period expires, the request is rejected.

If the request arrived within the ticket validity period, WebFOCUS validates the name of the requesting application, as described in the trusted ticket request validation. If the name provided by the IBIB\_appname parameter is not on the Application List, the trusted sign-on request is rejected. If the trusted sign-on request does not include the IBIB\_appname parameter, and no default application is identified, the request is rejected.

If the trusted sign-on request passes the validation, WebFOCUS retrieves and decrypts the IBIB\_userid, IBIB\_appname, and IBIB\_useripaddr parameters from the trusted ticket.

If WebFOCUS cannot find an existing account for the user ID identified in the IBIB\_userid parameter, it identifies the value in the Account Creation on Sign In setting. If this value is All, a new account for the user is created automatically. This setting can also use the value Off, or Mapped External Groups. For additional information on these configuration options, see [AUTOADD](#) on page 328.

If the trusted ticket includes the IP Address of the user in the IBIB\_useripaddr parameter, and the Client IP Matching check box for the Embedded BI Application is selected, WebFOCUS ensures that the IP address from the trusted ticket matches the IP address of the browser of the Embedded BI Application user who initiated the trusted ticket request. If the IP addresses do not match, the trusted sign-on request is rejected. If the IP addresses match, the trusted sign-on request is accepted.

If WebFOCUS accepts the trusted sign-on request, it opens a session for the user, and directs that user to the destination identified in the IBIB\_Destination parameter. The Embedded BI Application can then request content and resources on behalf of this user from WebFOCUS through URL requests or the WebFOCUS RESTful Web Services API.

If the Embedded BI Application must make POST requests that create or update WebFOCUS resources, a Cross-Site Request Forgery (CSRF) token must be obtained from WebFOCUS and submitted with these requests. Typically, the response to a Trusted Sign On Request returns XML that contains a CSRF token name and value pair that can be used for the session.

### **Using the Alternate Security Zone for Trusted Ticket Authentication**

In general, there is no requirement to enable the Alternate Security Zone to support the deployment of Embedded BI Applications. If it is not required, the Alternate Security Zone should remain disabled because it can complicate troubleshooting for trusted ticket authentication configurations.

However, if the Alternate Security Zone must be enabled while supporting trusted ticket authentication, WebFOCUS will first determine if a client request should be processed by the Alternate Security Zone configuration. By default, the Alternate Security Zone is configured to capture requests made to the localhost IP addresses 127.0.0.1 and 0:0:0:0:0:0::1. To create this configuration, enable trusted ticket authentication on the Alternate Security zone, and add the IP address of the host where the Embedded BI Application resides.

### Trusted Ticket Authentication Configuration Overview

The configuration of trusted ticket authentication requires administrators to configure the Embedded BI application and WebFOCUS to exchange information and authenticate Trusted Ticket requests and Trusted Sign-On requests.

To prepare the Embedded BI Application to support trusted ticket authentication, an Embedded BI Application developer must:

1. Configure the Embedded BI Application to issue a backchannel request for a trusted ticket to WebFOCUS that includes required identification information for that application.
2. Configure the Embedded BI Application to issue a front channel sign-on request using the trusted ticket by identifying the address of the WebFOCUS host.

For more information about how to configure the Embedded BI Application to make a trusted ticket request and a trusted sign-on request, see the *TIBCO WebFOCUS Embedded Business Intelligence User's Guide*.

This configuration and the information identification delivered by the Embedded BI Application must be available before an administrator can add the external application to the Trusted Ticket configuration within WebFOCUS.

To prepare WebFOCUS to support trusted ticket authentication, an administrator must:

1. Enable and configure trusted ticket authentication for the Security Zones that will support the Embedded BI Application.
2. If the Embedded BI Application and WebFOCUS are accessed from different origins, configure Cross-Origin settings for the security zone that will support Embedded BI Applications. For more information, see [Configuring Cross-Origin Settings](#) on page 159.
3. When the configuration is complete, restart Tomcat to enable WebFOCUS to accept trusted ticket connections.

## Evaluating Trusted Ticket Authentication

The Fintoso Embedded BI demo, which you must install in `drive:\jbi\WebFOCUS82\samples\embedded_demo`, includes the following two pages that can help you evaluate the Trusted Ticket feature:

- ❑ Create a Trusted Ticket Page:

`http(s)://host:port/embeddemo/tester/create_trusted_ticket.jsp`

- ❑ Test a Trusted Ticket Sign-on Request:

`http(s)://host:port/embeddemo/tester/test_trusted_ticket.jsp`

where:

*host*

Is the name or IP address of the host used to access WebFOCUS.

*port*

Is the number of the port on which the Web Server or Application Server listens.

This value is optional, and it should be excluded if the URL uses the default port for the protocol it uses in the scheme, which is port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

These pages identify the required and optional fields for each of the two transactions.

For more information about these two pages, see the *TIBCO WebFOCUS Embedded Business Intelligence User's Guide*.

**Note:** The address of the machine that hosts the browser that issues the request to the `create_trusted_ticket.jsp` page must appear in the Application List of the Edit Trusted Ticket Authentication Settings dialog box. If this address does not appear, the Create a Trusted Ticket page will not accept the request to create a trusted ticket. For more information about adding the address to this list, see [How to Configure Trusted Ticket Authentication](#) on page 316.

## **Procedure:** How to Configure Trusted Ticket Authentication

Before you begin, complete the prerequisites for Pre-Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

There may be additional prerequisites, such as configuring WebFOCUS for SSL. For an introduction to the steps required by this configuration, see [Configuring TIBCO WebFOCUS for SSL](#) on page 51. For information about other prerequisites, contact Customer Support.



Work with the developer of the Embedded BI Application to configure it to support a trusted ticket request and a trusted sign-on request. For more information, see the *TIBCO WebFOCUS Embedded Business Intelligence User's Guide*.

We also recommend that you use the Export command to back up the Security Settings configuration files before making changes to the Authentication page. For more information, see [How to Export Security Configuration Files](#) on page 171.

1. In the Administration Console, click the *Security* tab.
2. On the Security page, under the Security Zones folder:
  - a. If you support Embedded BI Applications in the *Default* Security Zone, under the Default Security Zones folder, click *Authentication*, and go to the next step.
  - b. If you support Embedded BI Applications in the *Alternate* Security Zone, under the Alternate Security Zones folder, click *Authentication*, and go to the next step.

**Note:** If you support Embedded BI Applications in both zones, configure trusted ticket authentication for the Default Security Zone first and then configure it for the Alternate Security Zone.

3. Click the Trusted Ticket Authentication entry, and in the Actions section, click *Edit*.

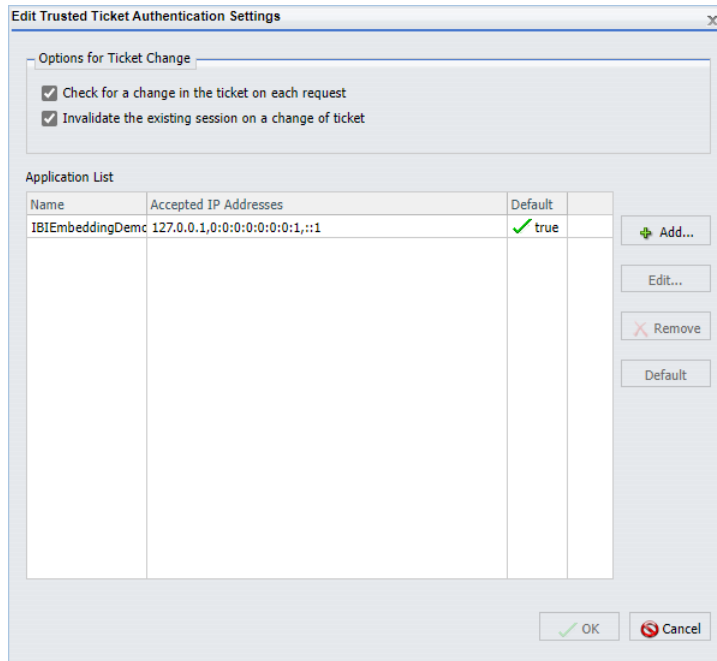
or

Right-click the Trusted Ticket Authentication entry, and then click *Edit*.

4. In the Edit Trusted Ticket Authentication Settings dialog box, accept the default selection of the Check for a change in the principal on each request check box and the Invalidate the existing session based on a change of principal check box.

These settings are configured to minimize the number of concurrent sessions by signing out an existing user when a new Trusted Ticket sign on request arrives during an open session and signing in the user that sent the new sign on request. We do not recommend that you clear these check boxes.

5. Click *Add*, as shown in the following image.



6. In the Application Settings for Trusted Ticket dialog box, type the name of the Embedded BI Application in the Application Name field, as shown in the following image.

Application Settings for Trusted Ticket

Application Name:

Alias of the Certificate: webfocus

Allowed Clock Skew (seconds): 60

The ticket validity period (seconds): 300

Trusted IP Addresses:

☐ Enable Client IP Matching

+ Add... Edit... ✗ Remove

✓ OK ✗ Cancel

Use the same spelling and capitalization as that of the application name that will be delivered in the HTTP Request message.

**Note:** To provide increased security, you can create a new certificate, add it to the WebFOCUS keystore, make an alias for it, and then click the name of that alias in the Alias of the Certificate list.

7. Click *Add*.
8. In the Add IP Address Pattern dialog box, type the IP address of the Embedded BI Application in the IP Address Pattern field.

You can use the IPv4 format, as shown in the following image.

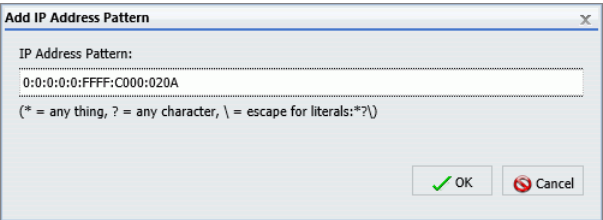
Add IP Address Pattern

IP Address Pattern:

(\* = any thing, ? = any character, \ = escape for literals:\*?)

✓ OK ✗ Cancel

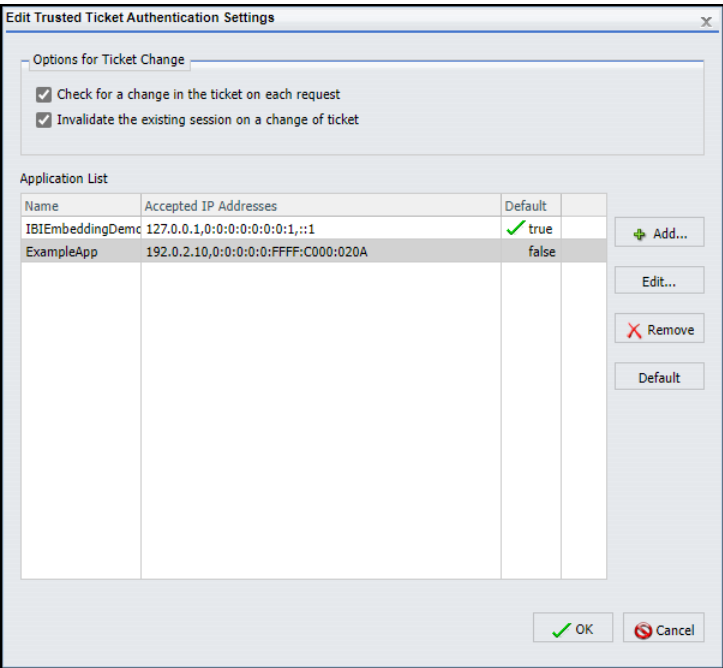
Or you can use the IPv6 format, as shown in the following image.



Type only one address in the IP Address Pattern field.

- 9. When you have entered your address, click **OK**.
- 10. If you need to add additional IP Addresses for the same application, repeat steps 7 through 9.
- 11. When you have entered all of the addresses you need, in the Application Settings for Trusted Ticket dialog box, click **OK**.

The new embedded application appears in the Application List, as shown in the following image.



- 12. If you need to add additional applications, repeat steps 5 through 11.

13. When you have entered all of the applications, in the Edit Trusted Ticket Authentication Settings dialog box, click *OK*.
14. On the Authentication page, in the Actions section, click *Save*.
15. When you receive a confirmation message, click *OK*.
16. When you receive the message to reload the web application, click *OK*.
17. Sign out of your current session.
18. Stop and restart the WebFOCUS Reporting Server.
19. Sign in again as an administrator and test the new configuration.

If the Embedded BI Application and WebFOCUS are deployed on two separate servers, configure WebFOCUS to Allow Embedding for the zones that support Embedded BI Applications. For more information, see [How to Allow Embedding for a Security Zone](#) on page 162.

If the Embedded BI Application must make POST requests that create or update WebFOCUS resources, establish cross-origin resource sharing for the zones that support Embedded BI Applications. For more information, see [How to Allow Cross-Origin Resource Sharing for a Security Zone](#) on page 165.

***Procedure:* How to Change the Name of the Cross-Site Request Forgery Token**

1. In the Administration Console, on the Configuration tab, under the Application Settings folder, click *Filters*.
2. On the Filters page, ensure that the *Cross Site Request Forgery Protection* check box is selected.
3. Ensure that the Cross Site Request Forgery Security Token field contains the value, *IBIWF\_SES\_AUTH\_TOKEN*.
4. Click *Save*.
5. In the Administration Console menu bar, click *Clear Cache*.
6. When you receive a confirmation message, click *OK*.

## External Authentication

In external authentication, a sign-in page is presented to users, who then type a user ID and password. The WebFOCUS Client passes these credentials to the WebFOCUS Reporting Server, which in turn validates them with an external source, such as Active Directory, LDAP directories, information in a custom RDBMS table, and web services. Users are authenticated externally both when they access the WebFOCUS Client, and when they access the Reporting Server browser interface directly.

**Note:** WebFOCUS does not currently support user password change through the WebFOCUS Reporting Server. Clear the *Enable Password Change* check box, located on the Advanced page of the Security tab, when configuring external authentication.

### Understanding Active Directory and LDAP Authentication

WebFOCUS can authenticate users to Active Directory and to LDAP directories by authenticating users to the WebFOCUS Reporting Server, and then using the WebFOCUS Reporting Server LDAP security provider to validate user credentials to the external directory.

Optionally, WebFOCUS can update the user account information in the WebFOCUS Repository with the email and description from the external directory.

### **Procedure:** How to Configure Active Directory and LDAP Authentication

Before you begin, complete the prerequisites for External Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

We also recommend that you use the Export command to save backup copies of the Security Settings configuration files before making changes to the Authentication page.

1. On the WebFOCUS Reporting Server, configure LDAP as the primary security provider and PTH as a secondary security provider.

For more information, see [Configuring a Security Provider on the TIBCO WebFOCUS Reporting Server](#) on page 30.

2. Sign in as an administrator, and open the Administration Console.
3. In the Administration Console, on the Security tab, under the Security Configuration folder, click *External*.
4. Select the *Enable External Security* check box.

The External page displays the settings currently assigned to the WebFOCUS Reporting Server.

5. Type *pth\srvadmin* in the Server Administrator ID field.
6. Type the password assigned to the Security User in the Password field.

The password for this account is pre-configured during the installation process to be the same as the password you supplied for the original administrator account.

7. Click *Connect*.

A confirmation dialog box opens, click *OK*.

8. In the User Authorization Group, click the *Internal* option.

9. In the *Account Creation on Sign In* list, click *Off*.
10. To update WebFOCUS accounts with the AD or LDAP user description and email during authentication, select the *Synchronize User Information with Authentication Provider* check box.
  - a. To retrieve updated user description and email information from the authentication provider, accept the default selection of the option, *With Authentication Provider*.
  - b. To retrieve updated user description and email information from the authorization provider, click the option, *With Authorization Provider*.

When your updates are complete your page will resemble the following image.

**External**

☒ **Enable External Security**

External Security Type: Reporting Server

Reporting Server Node: EDASERVE Refresh

Server Administrator ID: pth\svradmin

Password: \*\*\*\*\* Connect...

**User Authorization**

☒ Internal ☐ Internal and External ☐ External Only

Account Creation on Sign In: All

☒ **Synchronize User Information**

☒ With Authentication Provider ☐ With Authorization Provider

11. In the Administration Console Menu bar, click *Close*.
12. In the Security Configuration section, click *Save*.
13. When you receive the confirmation message, click *OK*.
14. When you receive the message to reload the web application, click *OK*.
15. Sign out of your current session.
16. Stop and restart the WebFOCUS Reporting Server.
17. Sign in as an administrator, and test the new configuration.

## Configuring Authentication by Information in an RDBMS Table

WebFOCUS can authenticate users against data in an RDBS table by using a CUSTOM security provider on the WebFOCUS Reporting Server. The CUSTOM provider uses a custom FOCUS procedure to perform the authentication. It is recommended that you store a hash of the user password in the RDBMS table and calculate the hash in your custom FOCUS procedure at run time before making the authentication comparison.

Optionally, user account information in the Repository can be updated with the email and description from the database.

### **Procedure:** How to Configure Authentication by Information in an RDBMS Table

Before you begin, complete the prerequisites for External Authentication. For more information, see [Configuring Pre-Authentication, External Authentication or External Authorization](#) on page 221.

We also recommend that you use the Export command to save backup copies of the Security Settings configuration files before making changes to the Authentication page.

1. On the WebFOCUS Reporting Server, configure a custom security provider as the primary provider and PTH as a secondary provider.
2. Sign in as an administrator, and open the Administration Console.
3. Click the Security tab, and on the Security page, under the Security Configuration folder, click *External*.
4. Select the *Enable External Security* check box.

The External page displays the settings currently assigned to the WebFOCUS Reporting Server.

5. Type a WebFOCUS Reporting Server Administrator account service user name in the Server Administrator ID field, using the format *ProviderName/serviceUserName*,

where:

*ProviderName*

Is the name of the RDBMS.

*serviceUserName*

Is the UserID for the RDBMS.

6. Type the password assigned to the Security User in the Password field.
7. Click *Connect*.

A confirmation dialog box opens, click *OK*.

8. In the User Authorization Group, click the *Internal* option.



If you are using the RDBMS to override other authorization methods, such as AD or LDAP, click the *Internal and External* option, and click the name of the RDBMS provider that will deliver authorization in the Group provider Override list.

9. In the Account Creation on Sign In list, click *Off*.
10. To update WebFOCUS accounts with the RDBMS user description and email during authentication, select the *Synchronize User Information with Authentication Provider* check box.

When your updates are complete your page will resemble the following image.

The screenshot shows the 'External' configuration page. At the top, there is a section 'Enable External Security' with a checked checkbox. Below this, there are fields for 'External Security Type' (set to 'Reporting Server'), 'Reporting Server Node' (set to 'EDASERVE'), 'Server Administrator ID' (set to 'pth\sradmin'), and 'Password' (masked with asterisks). There are 'Refresh' and 'Connect...' buttons. Below this is a 'User Authorization' section with three radio buttons: 'Internal' (selected), 'Internal and External', and 'External Only'. At the bottom, there is an 'Account Creation on Sign In' dropdown set to 'OFF' and a 'Synchronize User Information' section with two radio buttons: 'With Authentication Provider' (selected) and 'With Authorization Provider'.

11. Sign out of your current session.
12. Stop and restart the application server.
13. Sign in again using an RDBMS User ID and Password.

If you are able to sign in, the external authentication configuration was successful.

## Understanding Authorization

Authorization is the process of determining the capabilities and access privileges of authenticated users or programs. WebFOCUS software offers several options for authorizing users. By default, it is configured for internal authorization, in which user functional capabilities and resource access are based solely on information stored in the Repository. It can also be configured for external authorization, in which user capabilities and access rights are based on information managed outside of WebFOCUS software.

External authorization can be based on:

- ❑ Groups, roles, and user profile attribute values retrieved from any directory that supports the Lightweight Directory Access Protocol (LDAP), including Microsoft Active Directory (AD).
- ❑ Data retrieved from a relational database management system (RDBMS).
- ❑ Data retrieved from any WebFOCUS Reporting Server data adapter, including information from a web service or an ERP system.

For additional flexibility, WebFOCUS can authorize some users internally and others externally. If internal user accounts do not already exist when externally authorized users sign in, WebFOCUS automatically creates them.

## Understanding Internal Authorization

By default, WebFOCUS is configured for internal authorization, in which functional capabilities and resource access for users are based solely on information stored in the Repository. Administrators create users and place them into groups using the Security Center. External applications can use the web services API to create users and groups and manage group membership.

Typically, security rules are associated with WebFOCUS groups, so the access rights of users depend on the groups to which they belong. However, it is also possible to create security rules for individual users in order to address special requirements.

Internal authorization is supported with any authentication method, including internal, external, and pre-authentication.

## Understanding External Authorization

When you configure WebFOCUS for external authorization, it uses the security providers configured on the WebFOCUS Reporting Server (WFRS) to query an external source for information about users when they sign in. The information can include their email addresses, their descriptions, and their external group memberships. The WebFOCUS Reporting Server then returns this information to WebFOCUS, where it is used to create or update user accounts and define user authorizations. The security provider also returns other external information about users and groups to WebFOCUS in support of administrative features, such as obtaining a list of all external groups or the list of users who belong to an external group.

**Note:** Some organizations manage authorization data externally in LDAP user profile attributes or roles, rather than using LDAP groups. WebFOCUS also supports this approach.

Some external authorization scenarios supported by WebFOCUS include:

- ☐ Pre-authentication with external authorization
  - ☐ Windows Authentication is used to identify users, who are authorized according to their Active Directory group membership.
  - ☐ Users are authenticated by a Web Access Management system and are authorized according to information stored in a relational database management system (RDBMS).
  - ☐ A Software as a Service (SaaS) application is integrated with WebFOCUS to provide users with a single sign on (SSO) experience. Users are authorized based on information retrieved from an RDBMS or a web service.
- ☐ External authentication and authorization
  - ☐ An LDAP directory is used to authenticate users and retrieve group or role information for authorization.
  - ☐ Users are authenticated and authorized by custom SQL stored procedures.

## EXTERNAL and EXTERNALONLY Options

There are two options for configuring how WebFOCUS groups are mapped to authorization data in an external directory. These options appear in the User Authorization group located in the Administration Console, Security tab. External page.

### EXTERNAL

Specifies that some WebFOCUS groups may be mapped and some groups may be unmapped. Users are authorized if:

- ☐ They are members of an external group that is mapped to a WebFOCUS group.
- ☐ They are explicitly placed in an unmapped WebFOCUS group.

This is the recommended setting if the External Security Type (IBI\_Authentication\_Type) is set to Reporting Server.

### EXTERNALONLY

Specifies that users are authorized only if they are members of an external group that is mapped to a WebFOCUS group.

Be careful when selecting this option. If you do not have an external authorization that has been mapped to the WebFOCUS Administrators group, you can be locked out of WebFOCUS.

To retain administrative rights over WebFOCUS when specifying the EXTERNALONLY authorization, you must do one of the following:

- ❑ After configuring the EXTERNALONLY option, sign in to WebFOCUS with the superuser account, map the Administrators group to an external group, and then sign in to WebFOCUS with a user that belongs to the external group.
- ❑ After initially configuring the EXTERNAL option, sign in to WebFOCUS with an administrator account, map the Administrators group to an external group, configure the EXTERNALONLY option, and then sign in to WebFOCUS with a user that belongs to the external group.

**Note:** When a parent group in WebFOCUS has an external mapping, a user must be a member of the parent group to be considered a member of its child groups, whether membership in the child is mapped or directly assigned.

### AUTOADD

WebFOCUS offers the option of automatically adding pre-authenticated and externally authenticated users to WebFOCUS, if the user accounts exist in the external source, but do not already exist in WebFOCUS. Automatically added users can successfully sign in to WebFOCUS. Users who exist in the external source, do not exist in WebFOCUS, and are not automatically added, are denied access to WebFOCUS.

In the Security Center, WebFOCUS accounts which have been automatically created during the sign-in process have a status of AUTOADD, instead of ACTIVE.

### Limitations When Configuring External Authentication With External Authorization

The following constraints apply when you configure external authentication with external authorization:

- ❑ A WebFOCUS installation can support only a single WebFOCUS Reporting Server node for external authentication, external authorization, or both.
- ❑ The same WebFOCUS Reporting Server security provider must be used for both authentication and authorization for any given user.

- ❑ When you do not specify the provider for a user account, it is treated as an account from the primary provider. To use multiple WebFOCUS Reporting Server security providers for authentication or authorization, prefix the WebFOCUS user ID with the secondary security provider name for any individuals associated with it. For example, if the WebFOCUS Reporting Server has two LDAP providers, a primary provider named ldap01 and a secondary provider named ldap02, then the user accounts ldap01\user1 and ldap02\user2 must be created in WebFOCUS as user1 and ldap02\user2, respectively.

### Special Considerations When Using User Profile Attributes for Authorization

To authorize users based on groups, roles, or user profile attribute values retrieved from an LDAP directory or Microsoft Active Directory, configure an LDAP security provider on the WebFOCUS Reporting Server. The WebFOCUS Reporting Server then retrieves information about users, groups, roles, or user profile attributes from the external user directory and passes it on to the WebFOCUS Client. This LDAP security provider can also be used to authenticate user credentials for the WebFOCUS Client.

Typically, LDAP and AD user directories maintain group membership information, which is made available to other applications to authorize users. However, some organizations rely on other information stored in the directory, such as roles or user profile attributes, to populate the attribute with the necessary authorization information. These attributes may be single-valued or multi-valued and are not required to have any relationship to other objects in the external directory. Each of these methods of authorization is supported.

**Note:** Depending on the vendor and version, the LDAP directory may require a user membership plug-in to support the full set of external authorization features in WebFOCUS. Active Directory supports user membership natively. For more information, contact your LDAP administrator.

The LDAP provider can be configured to retrieve the authorization data from a user profile attribute and pass it back to WebFOCUS for authorization, as shown in the following image, where the ldap\_user\_group\_attribute AbcCorpRole is used to authorize users.

**Connection**

**User Search**

ldap\_user\_base?  Sample: dc=ibi,dc=com

ldap\_user\_scope?

ldap\_user\_class?

ldap\_user\_attribute?

ldap\_user\_group\_attribute?

Optional User Information

ldap\_user\_description?

ldap\_user\_email?

Since there is no corresponding directory object for the custom attribute, as there is with LDAP groups, the following limitations apply:

- ☐ The WebFOCUS Security Center will not show which users belong to WebFOCUS groups mapped to custom attributes.
- ☐ In the Security Center, the Browse button in the Edit Group dialog box does not allow you to search for custom attribute values. However, you can manually enter the attribute values.

## Configuring External Authorization

Setting up external authorization consists of the following steps:

1. Configure a security provider or providers on the WebFOCUS Reporting Server for the external source you will use for authorization. The security provider may be LDAP, Active Directory, or a custom provider, such as a provider that authorizes users to a relational database management system (RDBMS) or a web service.
2. Configure WebFOCUS to use the WebFOCUS Reporting Server for external authorization.
3. Restart the WebFOCUS web application.
4. Map WebFOCUS groups to external authorization data.

**Procedure: How to Configure TIBCO WebFOCUS for External Authorization**

Before you configure WebFOCUS for external authorization, you must have already configured the external authorization source as a security provider on the WebFOCUS Reporting Server. We strongly recommend that you also configure a trusted connection between the WebFOCUS Client and the WebFOCUS Reporting Server.

For more information on configuring security providers, see [Configuring a Security Provider on the TIBCO WebFOCUS Reporting Server](#) on page 30. For more information on configuring trusted connections, see [How to Configure the WebFOCUS Client to Make a Trusted Connection to the TIBCO WebFOCUS Reporting Server](#) on page 49.

1. In the Administration Console, on the Security tab, under the Security Configuration folder, click *External*.
2. Select the *Enable External Security* check box.  
  
The External page displays the settings currently assigned to the WebFOCUS Reporting Server.
3. Type a WebFOCUS Reporting Server Administrator account service user name in the Server Administrator ID field, using the format *ProviderName\serviceUserName*.
4. Type the password assigned to the Security User in the Password field.
5. Click *Connect*.
6. When you receive a confirmation message, click *OK*.
7. To update accounts in WebFOCUS with the AD or LDAP user description and email during authentication, select the *Synchronize User Information with Authentication Provider* check box.
8. In the User Authorization group, click *External Only* to assign all authorization tasks to an external provider, or *Internal and External* to share authorization tasks between WebFOCUS and an External Provider.
9. Save your changes.
10. In the Security Configuration section, click *Save*.
11. When you receive the confirmation message, click *OK*.
12. When you receive the message to reload the web application, click *OK*.
13. Sign out of your current session.
14. Stop and restart the WebFOCUS Reporting Server.
15. Sign in as an administrator, and test the new configuration.

16. Optionally, enable security tracing to help troubleshoot any issues with the new configuration.

- ❑ If you installed Apache Tomcat with WebFOCUS, make a backup copy of the `drive:/ibi/WebFOCUS82/webapps/webfocus/WEB-INF/classes/log4j.xml` file, then edit the `log4j.xml` file to change the level value for `com.ibilog` from *info* to *trace*.
- ❑ If you deployed the WebFOCUS web application from the web archive using the `webfocus.war` file, you can edit the `log4j.xml` file in its original location, then re-create the `webfocus.war` file.
- ❑ Alternatively, if you deployed the WebFOCUS web application from the web archive using the `webfocus.war` file, you can edit the `log4j.xml` file in its deployed location within the expanded directory. Check with your Java application administrator if you are unsure of this location or if you do not have access rights to modify the `log4j.xml` file.

17. Stop and restart the web application.

**Note:** Before restarting, you may wish to delete or rename the `drive:/ibi/WebFOCUS82/logs/event.log` file so that you will have a clean log file when WebFOCUS restarts in external authorization mode.

18. Sign in using the user account you created earlier.

**Tip:** The `event.log` file displays the external authorization information retrieved from the WebFOCUS Reporting Server security provider.

If you enabled security tracing in step 16, the `event.log` looks like the following example:

```
-WFRS.authenticate userName:userName
- EDA.authConnect node:EDASERVE User:userID
security:EXPLICIT-DYNAMIC
- EDA.authConnect node() provider:null reqName:userID
- edaAuth for node:EDASERVE user:userID returned:1000
- edaAuth for user:userID returned email:userEmail
- edaAuth for user:userID returned description:userDescription userID
- EDA.getGroupsForUser() node:EDASERVE userName:userID
- EDA.getGroupsForUser() provider:null reqName:userID userID
- group 1=#WF-ALL description=WF-ALL MAILING LIST userID
- group 2=#SharePointSiteAdmins description=SharePoint Admins userID
- group 3=#Summit_Lab_Staff description=#Summit_Lab Mailing List userID
- group 4=CORP-WF-DEV description=WF Product Team userID
- EDA.getGroupsForUser() from provider:null group count:4 userID
- User:userID has 4 external groups
```

If you were not able to sign in, try the account specified in the Root User (`IBI_Admin_Name`) setting.

You can now map WebFOCUS groups to external authorization data.



## Group Mapping

Mapping is the process of associating a WebFOCUS group with external authorization data, including external group memberships, external user profile data, or user information stored in an RDBMS. External authorization can be based on:

- ❑ Groups, roles, and user profile attribute values retrieved from any directory that supports the Lightweight Directory Access Protocol (LDAP), including Microsoft Active Directory (AD).
- ❑ Data retrieved from a relational database management system (RDBMS).
- ❑ Data retrieved from any WebFOCUS Reporting Server data adapter, including information from a web service or an ERP system.

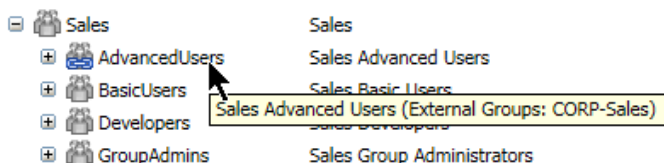
When WebFOCUS is configured for external authorization, individual WebFOCUS groups can be either mapped or unmapped.

**Note:** Mapping WebFOCUS groups to external authorization data requires the Group Mapping privilege (opExternalGroupMapping). By default, this privilege is assigned only to members of the Administrators group.

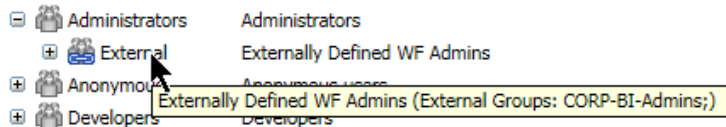
You can configure the authorization data used in the mapping through the Security Center or you can set external authorization attributes programmatically through a web service. For more information on using a web service, see the *WebFOCUS RESTful Web Services* section of the *TIBCO WebFOCUS® Embedded Business Intelligence User's Guide*.

The mapping is a property on a WebFOCUS group. The value of the property is a text string specifying the authorization data attribute in the external directory. To map a WebFOCUS group to multiple external groups or role attribute values, you can delimit the values with semi-colons (;) or use a wildcard symbol to match multiple external groups. For example, mapping a WebFOCUS group to `SALES-*` will map the WebFOCUS group to any external group beginning with `SALES-`. The text string may be up to 2,000 characters, including semi-colons (;).

The Security Center indicates mapped groups with a blue chain icon next to the group name. The tooltip for the group name displays the external data or user attribute to which it is mapped. The following image displays a configuration where a WebFOCUS group, the Sales/AdvancedUsers group, is mapped to an external group called CORP-Sales, but the other Sales subgroups are unmapped.



If members of a WebFOCUS group must be defined both internally in WebFOCUS and externally by a security provider, you can use an unmapped group for the internally authorized members and a mapped subgroup for the externally authorized members. The following image shows an example where the WebFOCUS Administrators group has a subgroup named External, which is mapped to the external group named CORP-BI-Admins.

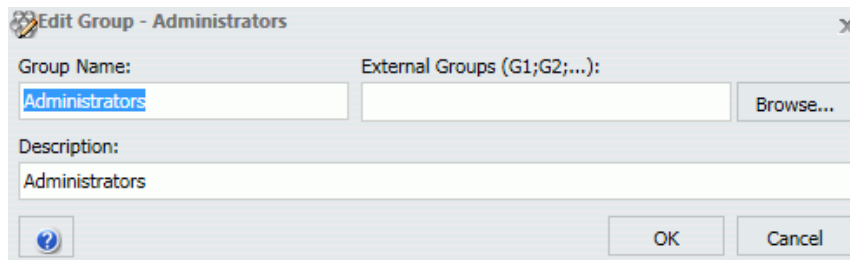


Members of both groups share the security policy of the unmapped parent group, while their memberships can each be managed separately.

### **Procedure:** How to Map TIBCO WebFOCUS Groups to External Authorization Data

1. In the Security Center, select the WebFOCUS group that you want to map to an external group and click *Edit Group*.

The Edit Group dialog box appears, as shown in the following image.

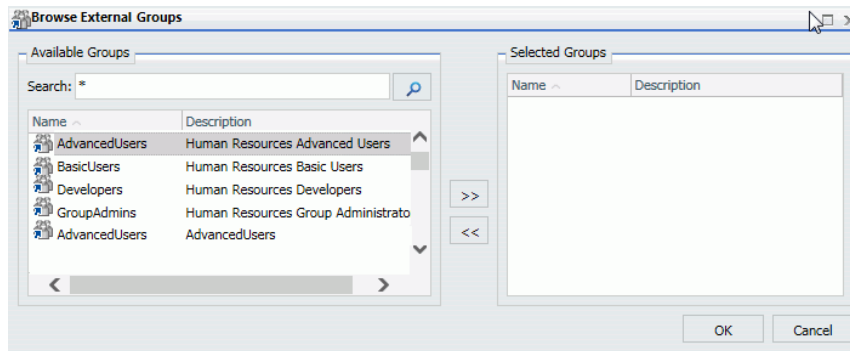


**Tip:** If the *Browse* button is not visible, WebFOCUS has not been configured for external authorization. For information on how to configure external authorization, see [How to Configure TIBCO WebFOCUS for External Authorization](#) on page 331.

2. If you know the value of the attribute to be used for external authorization, you can enter it manually. Otherwise, click *Browse*.

**Note:** If you want to use a custom user profile attribute for authorization, you must enter the value manually.

The Browse External Groups dialog box appears, as shown in the following image.



3. Enter the search term and click *Search*.

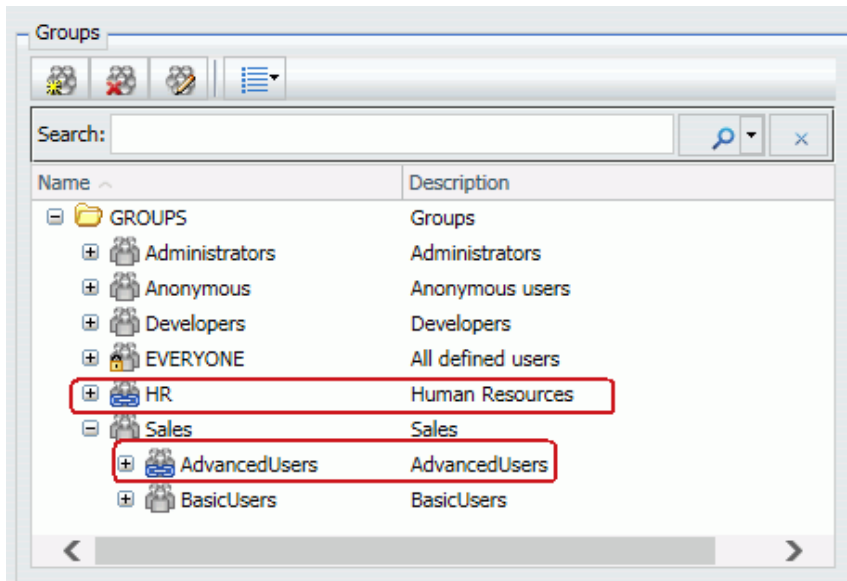
**Note:** By default, WebFOCUS searches only the primary security provider. To look up data using a secondary security provider, you must include the provider name in your query. For example, to find Sales groups for a secondary PTH provider, you would search for *PTH \\*Sales*. To find all groups for all security providers, search for *\*\\**.

4. Select the values to which the WebFOCUS group will be mapped and click *OK*.

**Note:** You can select multiple values.

5. When you return to the Edit Group dialog box, the external groups you have selected appear in the External Groups field. Click *OK* to save your changes.

When you return to the Security Center, the mapped group appears with a link icon, as shown in the following image.



When you mouse over the group, the tooltip displays the mapped external authorization data in parentheses after the WebFOCUS group name.

## Special Considerations for Microsoft Office Drill-Down Links

When you select a Microsoft Office product as the target of a drill-down link, the drilldown will fail because the targeted product was launched outside of the browser. The security context and previously-established session-related cookies, along with the user authorization that was based on them, are not retained in the targeted product.

The drill-down feature in WebFOCUS Release 7.7.x functioned in Microsoft Office products because anonymous drill-down access was permitted. To enable the use of this feature in WebFOCUS Release 8.x, select one of the following options that best suits your organization:

- ☐ Add the ForceShellExecute subkey to the registry of the machine that hosts the Application Server, and set the Value to 1.

This registry change overrides the default URL handling method used by Excel and has ramifications beyond WebFOCUS.

For more information on how to update the registry and how Microsoft Office products work with session-related information, see the Microsoft Office support site at:

<http://support.microsoft.com/kb/218153>

- ☐ Configure WebFOCUS security to give the public user the necessary permissions to drill down to reports.

This option requires you to make the content that is targeted by the drill-down link available to public users, which is not suitable to any customer who wishes to maintain even a minimal level of content security.

- ☐ Enable the Remember Me feature on the Sign in page. If the end-user chooses the Remember Me feature, a persistent cookie is established.

The Remember Me feature does not consistently produce a successful log-in, and the persistent cookie could inadvertently create a new session that could cause processing problems for applications that rely on the foccache directory. The auto log-in functionality could also introduce unacceptable vulnerabilities to security-conscious customers.

- ☐ Use Single Sign-On (SSO) with IIS/Tomcat Integrated Windows Authentication. A renegotiation of the sign-in credentials occurs automatically, and the Excel report displays correctly.

Depending on the SSO system, users may not be logged in to a new session automatically, and the new WebFOCUS session can cause issues for applications that rely on the foccache directory.

## Special Considerations for TIBCO WebFOCUS Deployments With Separate ReportCaster Installations

When the ReportCaster Distribution Server and the WebFOCUS Client are installed on separate machines, ReportCaster does not have access to the WebFOCUS configuration files that are updated through the Administration Console. To ensure that WebFOCUS configuration changes are available to ReportCaster, you must perform additional configuration steps. This is especially critical when configuring external authentication or authorization because ReportCaster jobs may not run properly if ReportCaster and WebFOCUS do not have the same security settings.

### ***Procedure:*** How to Configure ReportCaster Distribution Server Settings to Match TIBCO WebFOCUS Client Settings

Once you have verified that the WebFOCUS configuration changes work properly, copy the configuration files from the machine on which WebFOCUS is installed to the machine on which the ReportCaster Distribution Server is installed.

1. If you have modified the WebFOCUS Client settings, copy the *drive:\ibi\WebFOCUS82\config\webfocus.cfg* file from the WebFOCUS machine to the *drive:\ibi\WebFOCUS82\config* directory on the ReportCaster machine.

2. If you have modified the settings for WebFOCUS Client connections to the WebFOCUS Reporting Server, copy the *drive:\ibi\WebFOCUS82\client\home\etc\odin.cfg* file from the WebFOCUS machine to the *drive:\ibi\WebFOCUS82\client\etc* directory on the ReportCaster machine.
3. If you have modified the Repository settings, copy the *drive:\ibi\WebFOCUS82\client\etc\install.cfg* and *webfocus.cfg* files from the WebFOCUS machine to the *drive:\ibi\WebFOCUS82\client\etc* directory on the ReportCaster machine.

If repository settings are not stored in *install.cfg*, this step is not necessary.

4. Restart the Distribution Server and test scheduled jobs to verify that they perform as expected.

## TIBCO WebFOCUS Administration

---

This topic explains how to develop and administer a security policy for your WebFOCUS installation. It introduces basic security concepts, describes the repository file structure, and defines the basic elements of the WebFOCUS security model, such as users, groups, roles, privileges, resources, security rules, and security policy.

### In this chapter:

- ☐ [Assessing Security Requirements](#)
  - ☐ [IBFS Filesystem and Subsystems](#)
  - ☐ [Components of the Security System](#)
  - ☐ [Policy Design](#)
  - ☐ [Working With Folders](#)
  - ☐ [Understanding Workspaces](#)
  - ☐ [Creating a Custom Resource Template](#)
  - ☐ [Understanding Access Control Templates](#)
  - ☐ [Working With Message Templates](#)
- 

### Assessing Security Requirements

Before you can design or implement a security policy, you must first define the security requirements of your organization. The following questions may prove helpful in the process of definition, even if they cannot cover every possible concern. You may also benefit from experimenting with the resource templates included in your installation to get an idea of the design possibilities supported by the software, even if you plan to develop a custom policy.

Security policy considerations include:

- ☐ Which groups of users have similar reporting and access requirements?

Often, these groups are departments in an enterprise deployment or tenant organizations in a SaaS deployment. There may also be overarching groups who have access to all resources in the Repository, such as the Administrators group or a centralized report scheduling organization.

- ❑ What reporting tools, privileges, and roles do users require?

For example, will users be creating their own reports, or are they only running prebuilt reports? Can users schedule reports, and if so, do they have access to all of the scheduling features or only a subset? Do managers need privileges not available to other users?

**Note:** Overcomplication can make a system more difficult for administrators to manage or users to understand. You may want to limit the number of roles you create, in the interest of streamlining the user and administrator experience.

- ❑ How many WebFOCUS environments will there be? How do requirements vary for different environments?

Enterprise deployments often have separate development, test, and production implementations of WebFOCUS, and may not include developer roles in the test and production environments. By contrast, in SaaS deployments, tenant developers may be developing new reporting content for their organizations directly in the production environment.

- ❑ Will you be deploying content inside a WebFOCUS BI Portal?

If so, will each department or tenant have its own portal, or will everyone access a single portal? It may be easier to manage a single enterprise portal, where some pages are available to everyone, and other department-specific or tenant-specific pages are available only to users in those organizations.

- ❑ Will your administrative model be centralized, or do you wish to delegate some responsibilities to group administrators?

For example, you can let a sales group administrator assign users to reporting roles, instead of making this the responsibility of the system administrator.

## IBFS Filesystem and Subsystems

WebFOCUS stores information about its resources in a relational database referred to as the WebFOCUS Repository. These resources are all organized in the IBFS Filesystem, a logical addressing system used to store and retrieve objects.



IBFS is hierarchical and is built on a set of subsystems that help organize the objects within the repository. Every object has a unique IBFS path. IBFS paths are used for many things, including maintaining group membership, controlling references to drill-down procedures, and checking whether users are authorized to access individual resources. In particular, security rules reference IBFS paths. The security policies created by these rules propagate down the IBFS path hierarchy through inheritance. This means that each subsystem inherits the policy of its parent, unless a new policy is specifically applied to the subsystem.

**Note:**

- ❑ The following characters are not permitted to be used within an IBFS path:

(Blank Space) & \* ( ) | : ; " , ?

- ❑ Although the slash mark (/) is valid within a path specification, it cannot be used in the name of a folder or item.

If you use restricted characters in the Title when creating a new folder or item, they are automatically removed from the Folder Name or File Name.

- ❑ We recommend that organizations working in a UNIX or Linux environment use lowercase characters when creating file and directory names for WebFOCUS Reporting Server resources, such as metadata or FOCEXECs.
- ❑ Don't use the term /bi as the main alias or context or at any other point within an IBFS path. This is a reserved term, and its use as an alias or context prevents the proper display of the Administration Console and Security Center.

If you are working from a view on the Hub, or with the WebFOCUS Home Page, right-click an item, and then click *Properties* to open the Properties panel.

The Properties panel displays the IBFS path of the object in the Path label, as shown in the following image.

Properties: Provider

General

Advanced

Server

Title

Provider

Name

Provider

Summary

Path

IBFS:/WFC/Repository/Provider

Created

Tuesday, December 7, 2021 5:12:23 PM EST by admin

Modified

Tuesday, December 7, 2021 5:13:22 PM EST by admin

Accessed

Tuesday, December 7, 2021 5:13:22 PM EST by admin

Owner

-

Publish

☒

Show

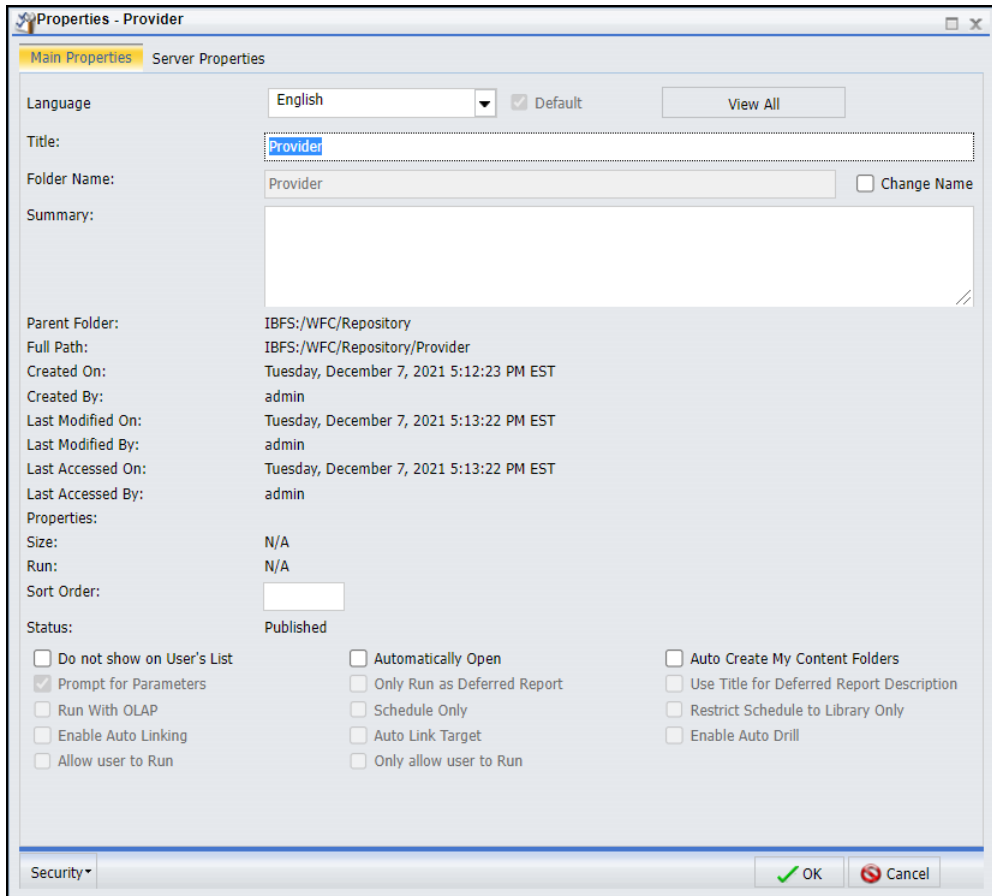
☒

Cancel

Save

If you are working with the Legacy Home Page, right-click an object, and then click *Properties* to open its Properties dialog box.

The Properties dialog box displays the IBFS path of the object in the Full Path label, as shown in the following image.



On the Legacy Home Page, the default view of the Business In8telligence Portal Resources tree is the Repository View, which displays elements with user-friendly labels. To view the IBFS subsystems in the Resources tree, right-click the Workspaces node, point to *View*, and then click *Full View*. To return to the Repository View, right-click the TIBCO WebFOCUS node, point to *View*, and then click *Repository View*.

**Note:** Use the Full View only for custom resource templates. For all other functions, use the default Repository View.

An IBFS path begins with the namespace designation IBFS: and is followed by an IBFS subsystem. Variables in the path dynamically select relevant resources based on the workspace, folder, group, and language of the user that calls the resource. Report procedures, schedules, and library content are all stored in the WFC subsystem.

Resources in the WFC subsystem have a Name and a Title. Name refers to the IBFS name of the object and Title refers to its display name in the Resources tree.

**Note:** The IBFS name of the Content node displayed in the Resources tree is Repository. This node is referenced by the IBFS path IBFS:/WFC/Repository.

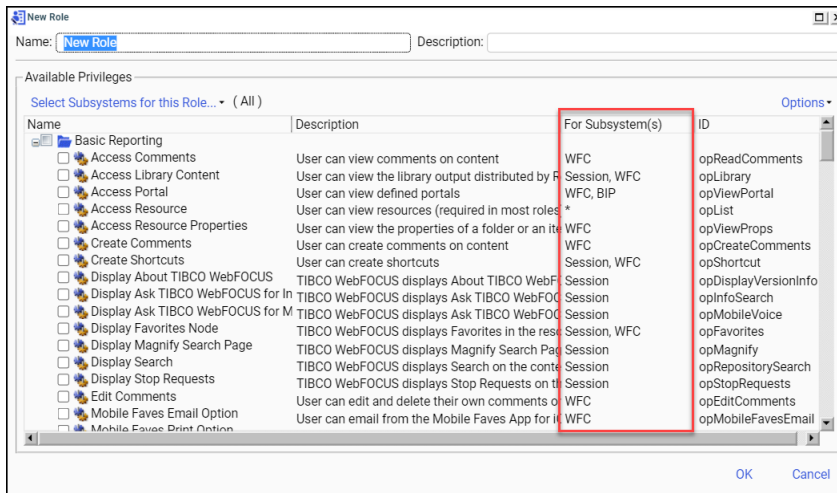
The USERS, GROUPS, and ROLES subsystems are all organized under the SSYS subsystem. In the GROUPS subsystem, the IBFS addresses of subgroups include the names of their parent groups, just as subgroups are nested under parent groups, as shown in the following image.



In the example above, an administrator has set up a Sales group with the subgroups AdvancedUsers, BasicUsers, Developers, and GroupAdmins. The IBFS path for AdvancedUsers is IBFS:/SSYS/GROUPS/Sales/AdvancedUsers.

The EDA and FILE subsystems reference resources outside of the Repository. You can set up rules for the EDA subsystem to hide specific WebFOCUS Reporting Server nodes from a group of users, or for the FILE subsystem to secure access to WebFOCUS file system-based resources, including the import and export directories under WebFOCUS\_installldir/cm.

When you create or view a role, each privilege it contains has a For Subsystem(s) column, as shown in the following image.



In addition to listing the subsystems to which the privilege applies, the For Subsystem(s) column also specifies whether the privilege is a session privilege, a local privilege, or a hybrid privilege.

**Note:** An asterisk (\*) in the For Subsystem(s) column indicates that the privilege applies to all subsystems.

## Using Variables in IBFS Paths

Most IBFS Paths point directly to a single end point within the Repository. However, developers may need to create paths for portals or other applications that can be directed to a contextually-appropriate resource instead of a single resource designed to serve all users.

For example, you can use variables in the IBFS paths of a portal to facilitate multi-tenancy with custom styling. Specifically, you can create a single portal that leverages the same base information, but delivers it to the users of each tenant application using a logo and color scheme that is applicable to their organization.

To accommodate dynamic IBFS paths, the repository contains a set of variables which, when preceded by two number sign (##) characters, substitutes a value presented by the user, such as group name or user name, and directs the user to a resource that conforms to the requirements of the group, folder, or other characteristic represented by the variable.

These variables include:

- ❑ **WF\_MyContentFolder.** Indicates that the variable is to be replaced by the MyContent folder of the user who invoked the IBFS Path.
- ❑ **WF\_PersonalFolder.** Indicates that the variable is to be replaced by the name of the UserInfo folder of the user who invoked the IBFS Path.
- ❑ **WF\_PrimaryGroup.** Indicates that the variable is to be replaced by the name of the first top level group in which the user who invoked the IBFS Path is a member.
- ❑ **WF\_Language2.** Indicates that the variable is to be replaced by the two-character (uppercase) language code of the user who invoked the IBFS Path.

Variable names are case insensitive.

### **Procedure:** How to Include a Variable in an IBFS Path

Use this procedure as a guideline when you must type a path to a resource that must vary by a specific characteristic presented by the user at run time. For example, you can use this procedure when typing a path to invoke the logo file or CSS theme file used by an individual tenant group when running a portal that is used by multiple tenant groups.

1. Begin the path with IBFS:/ and type the names of the workspace and folders in the path, each separated by a slash mark (/), until you reach the level where the path should point to a folder or other resource that depends upon a characteristic presented by the user at run time.

For example: IBFS:/Sales/Month

2. When you reach the level at which the path must vary according to the characteristic presented by the user, type the relevant variable in the following format:

`##{variablename}`

where:

*variablename*

Is a variable that represents a characteristic about the user who invoked the IBFS Path by running a procedure or portal. For a list of variables see [Using Variables in IBFS Paths](#) on page 345.

For Example: IBFS:/Sales/Month/##{WF\_PrimaryGroup}

**Note:** Variable names are not case sensitive.

3. If the same path is used below that level, continue the path from the variable to the name of the resource at the end point.

For example: IBFS:/Sales/Month/##{WF\_PrimaryGroup}/Hidden\_Content/theme.css

4. Test your path to ensure that it directs users with varying credentials to the appropriate resources.

## Components of the Security System

The basic components of the security system are privileges, resources, and rules. The security policy for each user is determined by the combination of rules that applies to that user for each specific resource. The rules control which privileges are available to each user under different circumstances. For example, a user may have the privilege to edit a resource in one folder, but not another.

### Privileges

A privilege controls access to a tool, resource, or ability. For example, different privileges control access to each of the following:

- ☐ Folders, which can contain procedures, Library content, Access Lists, Schedules, and other resources.
- ☐ Shortcut menu options, such as the ability to run a procedure or delete a folder.
- ☐ The Administration and Tools menus, within the menu bar, and menu items within them.
- ☐ Resources tree nodes, which enable access to resources such as portals, change management packages, and WebFOCUS Reporting Servers.
- ☐ The list of users available within the Security Center to a group administrator in an enterprise deployment or to a tenant administrator in a SaaS deployment.

Similar privileges are grouped into roles so they can be used in security rules. Privileges and roles are used in rules that associate users and groups with resources. For example, you might want to create a role containing all the privileges you wish to grant basic users or a role containing all the privileges you wish to grant developers.

For a list of all privileges, see [Privileges](#) on page 635.

### Types of Privileges

When you are creating or modifying roles or rules, it is important to understand what the privileges involved do, how they are used, and where they apply.

## Local Privileges

Local privileges define functional capabilities that users can be assigned on one or more subsystems. Local privileges are used to enable shortcut menu choices, such as *Run* on a report or *Delete* on a folder. Local privileges also determine which items are shown inside tools, such as which users are displayed inside the Security Center or which schedules appear in ReportCaster. For example, group managers may be permitted to see only users in the groups they manage, rather than all the users in the system.

Local privileges are evaluated for each user at every level within a subsystem. They can be permitted for a user on one folder and denied on another. For example, a user might be permitted Access Resources and Run Procedures on the Sales workspace folder but denied these privileges on a subfolder. The user could run reports in the Sales folder but could not see the subfolder or run reports inside it. When users belong to multiple groups, they may be permitted a local privilege in one group and denied the privilege in another. In such cases, the users are denied the privilege.

Local privileges are evaluated when features such as tree controls or tool UIs are rendered. Changes to local privileges take effect immediately, but users may need to refresh or reload the interface to see the changes. For example, if the Access Resource privilege on the Sales subfolder is granted to a user who was previously denied the privilege, the user may need to refresh the display of the Sales folder in order for the subfolder to appear.

In the Security Center, local privileges have one or more IBFS subsystem names listed in the For Subsystem(s) column. An asterisk in this column means that the local privilege can be used with any subsystem.

## Session Privileges

Session privileges define functional capabilities that users can be assigned during the sign-in process. Session privileges are used to enable menu bar drop-down list items, nodes on the Resources tree, and other global user capabilities, such as many of the buttons in the desktop products.

Session privileges are evaluated for each user when they sign in. The rules that are set on the Workspaces node (WFC/Workspaces) and on subfolders beneath it to the depth specified by the Session Privilege Search Depth (IBI\_SESSION\_PRIVILEGE\_SEARCH\_DEPTH) setting are evaluated. The default value is 1, which means that, by default, the evaluation only looks for session privileges on workspace folders immediately under the Content node.



**Note:** As you increase the Session Privilege Search Depth (IBI\_SESSION\_PRIVILEGE\_SEARCH\_DEPTH) setting, the evaluation searches deeper into the repository for resources accessible to the user during sign-in. This may increase the amount of time it takes to process sign-in operations. To prevent performance issues, we strongly recommend that the Session Privilege Search Depth (IBI\_SESSION\_PRIVILEGE\_SEARCH\_DEPTH) setting be no greater than 2. For more information about the Session Privilege Search Depth (IBI\_SESSION\_PRIVILEGE\_SEARCH\_DEPTH) setting, see *BI Portal Settings*.

When session privileges conflict (for example, when a user is permitted a session privilege because of membership in one group and denied the privilege because of membership in another), users are permitted the privilege. For example, a user who is permitted Display Favorites Node (opFavorites) because of membership in one group and denied it because of membership in another will be permitted the privilege, enabling the user to see the Favorites node on the Resources tree.

**Note:** This is the opposite of the resolution of conflicts for local privileges, where privileges that are both permitted and denied are evaluated as denied.

Changes made to session privileges take effect the next time a user signs in.

In the Security Center, session privileges are listed as *Session* in the For Subsystem(s) column.

## Hybrid Privileges

A privilege that is both a local privilege and a session privilege is a hybrid privilege. Hybrid privileges are used for dual purposes: to enable some global capability and to optionally enable local capabilities within a subsystem.

For example, the hybrid privilege Run Procedures Deferred is listed as Session, WFC. The session privilege part of this hybrid privilege is used to determine whether to show Deferred Status in the Tools menu, and the local privilege is used to determine whether to enable the Run Deferred option on the shortcut menu of procedures under the Workspaces node.

In a typical deployment where the Session Privilege Search Depth (IBI\_SESSION\_PRIVILEGE\_SEARCH\_DEPTH) setting is 1, rules that include hybrid privileges should be permitted on at least one top-level workspace folder, although they can also be denied on other top-level folders or on subfolders. This configuration prevents the situation in which a user is able to run a procedure deferred, but is subsequently unable to retrieve the output from the deferred request.

In the Security Center, hybrid privileges are listed with *Session* and one or more subsystems.

Resources

A resource is any folder, item, library content, portal, privilege, report procedure, role, user, or group to which access can be controlled or to whom abilities can be granted.

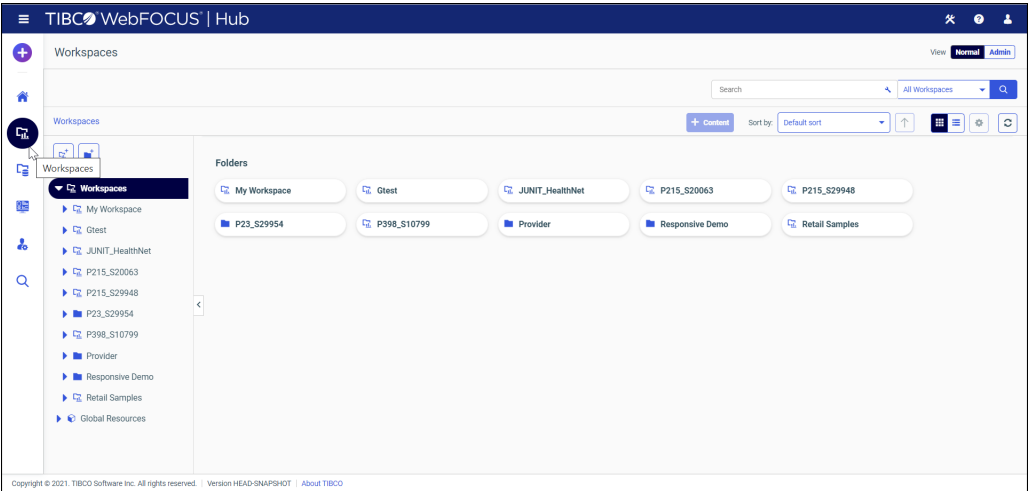
Different resource types have different controlled privileges. For example, all resource types can be deleted, but report request resources cannot be made members of a group and user resources cannot be run or scheduled.

Users gain access to resources from items listed on the Resources tree or displayed in the content area. For customers with legacy licenses, the visibility of licensed components depends upon the license key installed with the product.

Viewing Resource Components

The most complete display of licensed components appears in the Workspaces area.

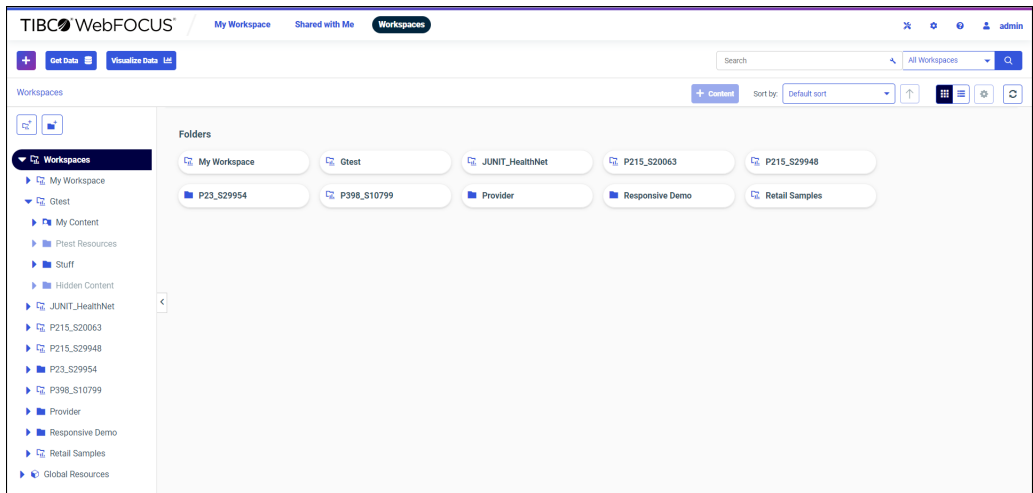
To open the Workspaces area directly from the Hub, select *Workspaces* from the side navigation pane, as shown in the following image.



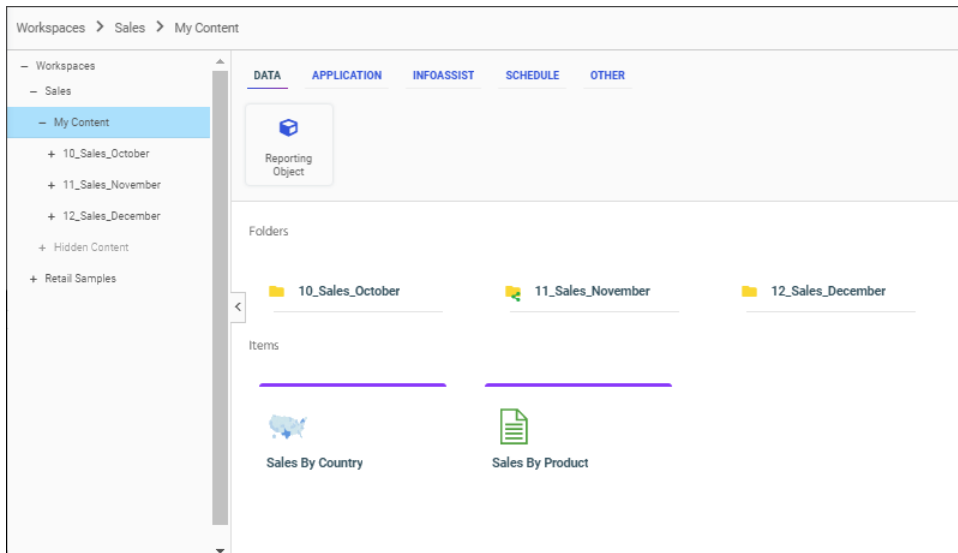
You can also open the Workspaces area from the WebFOCUS Home Page by selecting *Workspaces* in the banner, as shown in the following image.



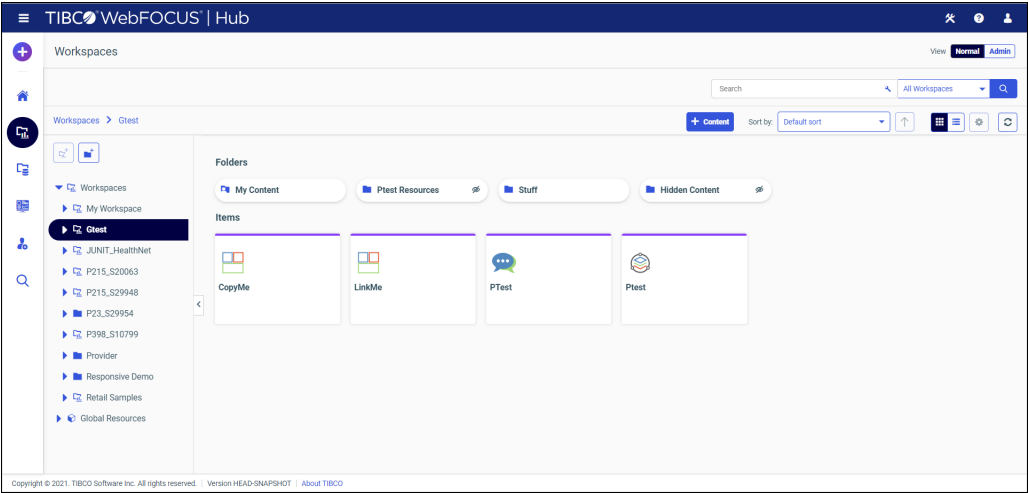
The WebFOCUS Explorer opens and displays links to existing workspaces and folders, as shown in the following image.



When you open a folder from the WebFOCUS Home Page, the WebFOCUS Explorer displays the items that folder contains, as shown in the following image.

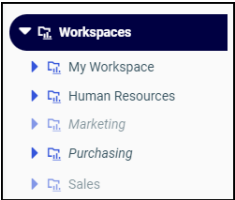


When you open a folder from the Workspaces view in the Hub, the WebFOCUS Explorer displays the items that folder contains, as shown in the following image.





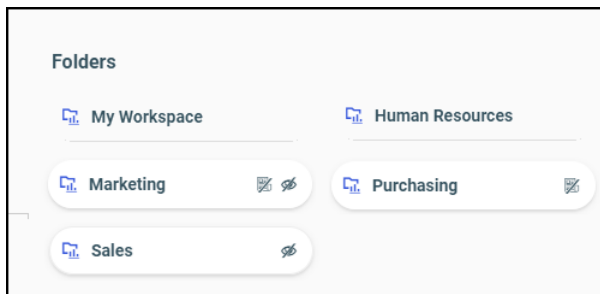
Visual cues indicate whether resource items are private or published, shown or hidden, shared or not shared. In the Workspaces area, resources that are shown are visible to users who are not able to use them to create content. Resources that are hidden are not visible to those users.


In the Resources tree, private workspaces are displayed in italics. Published workspaces are not. Hidden workspaces are dimmed. Workspaces that are to be shown are not dimmed. These variations are shown in the following image.





In this example, the Human Resources entry is not dimmed and does not use italics. The folder it represents is published and is shown. The Marketing entry is dimmed and uses italics. The folder it represents is private, and is hidden. The Purchasing entry is not dimmed but uses italics. The folder it represents is private, and is shown. The Sales entry is dimmed and does not use italics. The folder it represents is published, and is hidden.


In the content area, the same conditions affect the display of items in similar ways. Private folders display a Private icon. The private icon pictures a published document with a strikethrough symbol . Published folders do not include this icon. Hidden folders include a Hidden icon. The hidden icon pictures an eye with a strikethrough symbol . Folders that are to be shown do not include this icon. These variations are shown in the following image.



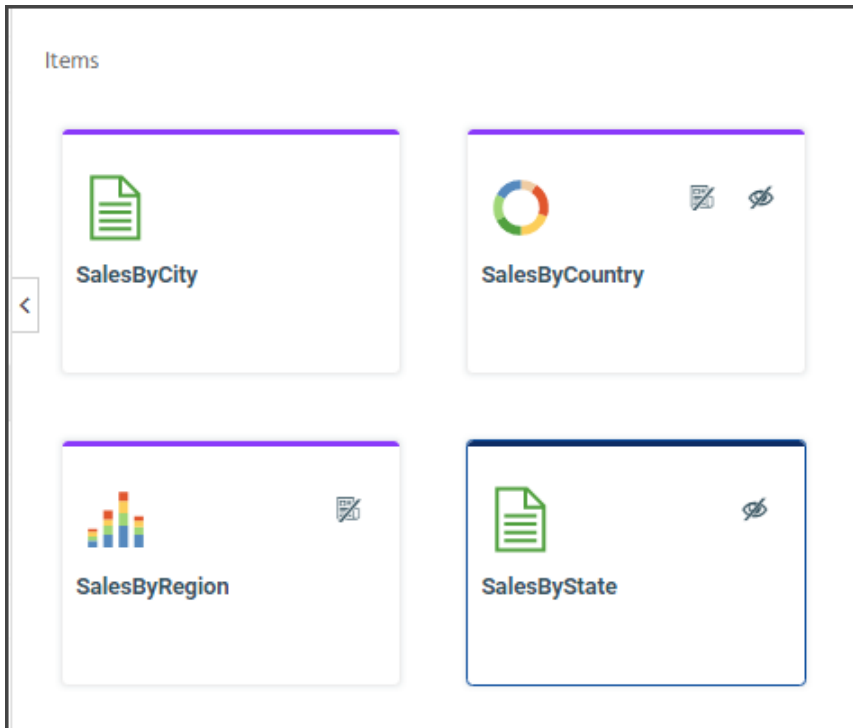
In this example, the Human Resources folder  displays no icons. The folder it represents is shown and published.

The Marketing folder  displays a hidden and private icon. The folder it represents is hidden and private.



The Purchasing folder  displays a private icon. The folder it represents is shown and private.

The Sales folder  displays a hidden icon. The folder it represents is hidden and published.

The same visual cues apply to items within folders, as shown in the following images.



In this example, the SalesByCity report shows no icons in the tile other than the thumbnail for the report itself. The report it represents is published and is shown.

The SalesByCountry chart shows a private icon and a hidden icon in the tile. The private icon pictures a published document with a strikethrough symbol.  The hidden icon pictures an eye with a strikethrough symbol.  The chart it represents is private, and is hidden.

The SalesByRegion item only shows a private icon in the tile next to the chart thumbnail. The chart it represents is private, and is shown.

The SalesByState report item only shows a hidden icon in the tile next to the report thumbnail. The report it represents is published, and is hidden.

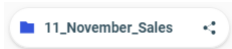
When you right-click a resource, the options presented to you are based on your privileges and the status of that item. When you right-click a published item, you are presented with the option to Unpublish it. If that item is private, you are presented with the option to Publish it.

You can also view the publish or show status of an item from the Properties dialog box. To open it, right-click the item in the Resources tree or content area and select *Properties*. The Yes option in the Publish setting is selected if the item is published, and the No option is selected if it is private. Similarly, the Yes option in the Show setting is selected if the item is to be shown to users who cannot use it to create content, and the No option is selected if it is to be hidden from those users.

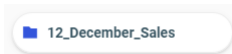
You can share private folders and resources in the My Content folder or in any sub-folder within it. Within the content area of these folders, shared resources are identified with a Shared icon



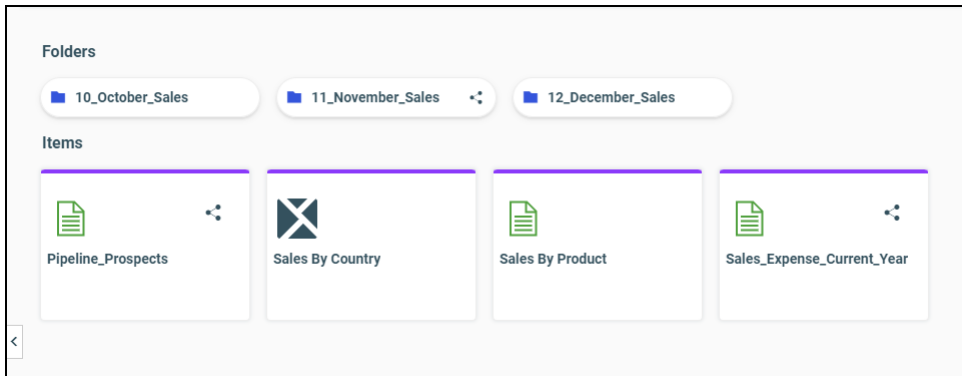
Icons for resources that are shared display this additional icon as an overlay



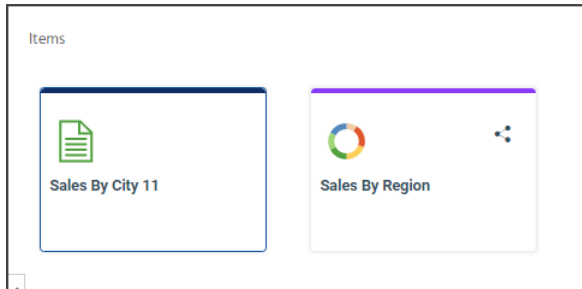
Icons for resources that are not shared do not display this additional icon



The overlay applies to folders and to individual items. As shown in the following image, the 11\_November\_Sales folder, the Pipeline\_Prospectors report, and the Sales\_Expense\_Current\_Year report are all shared.



As shown in the following image, the Sales By Region chart is shared, but the Sales By City report is not shared.



**Note:** Tiles representing resources configured to Run With Insight will also include the Run With Insight icon, as shown in the following image.



The Run With Insight icon  represents an index finger selecting a button or onscreen option. For more information, see the *TIBCO WebFOCUS® User's Guide*.

### User and Group Resources

A user is identified by a unique ID and may also have additional properties, such as description, email address, password, group memberships, and active, inactive, or AUTOADD status. Groups are formed of users or subgroups, in which all members require similar capabilities or access to the same resources. All users are members of the EVERYONE group, which is the set of all named users in the system.

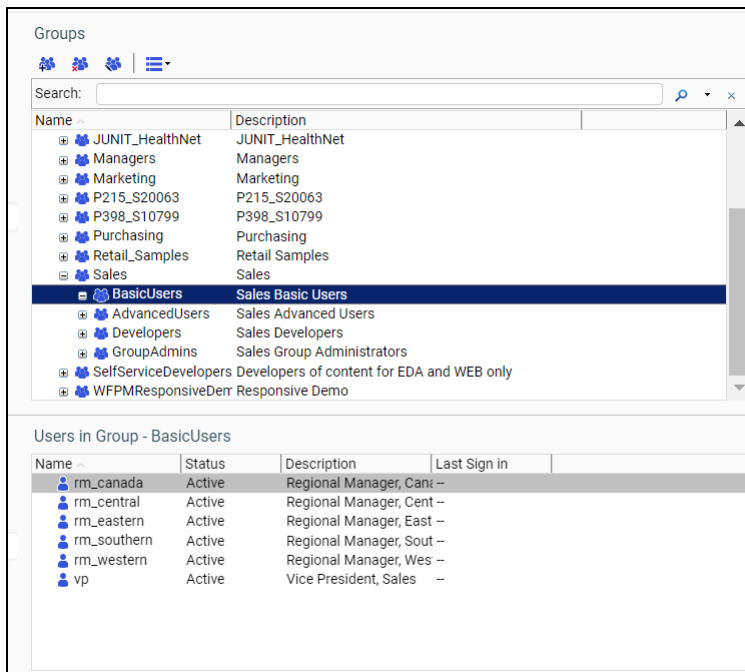
**Note:** In multi-tenancy SaaS deployments, although tenant users belong to the EVERYONE group along with the service provider users, the tenant users are only aware of other users within their own organization.



## Explicit and Implicit Groups

The groups to which a user is assigned are called explicit groups. Users always have at least one explicit group because they all belong to the EVERYONE group. Groups can also be nested in a hierarchy to simplify administration. In the hierarchy, if a subgroup is nested in a parent group, the users who are members of the subgroup are considered to be members of the parent group. The subgroup is an explicit group for its members and its parent group is an implicit group.

In the following image, the Sales group is the implicit group, and the BasicUsers group under Sales is the explicit group.



Security rules apply to both implicit and explicit groups. That is, rules which apply to the implicit group also apply to the explicit group nested in it.

**Note:** In multi-tenancy SaaS deployments, the EVERYONE group and its members are not visible to tenant users.

### Private and Published Resources

Content resources, such as portals, reports, and procedures, are either private or published. Private content is available only to the owner and authorized users with whom it is shared. Published content may also be shared with authorized users, but user access to published content is controlled by rules, rather than the individual decision to share it. Published content is considered authoritative and has usually undergone quality assurance and testing before being published for the user community.

#### *Private Resources*

All resources are initially created as private resources. The security policy for private resources specifies the following:

- ☐ The owner of the resource is the user who created the resource.
- ☐ The resource does not inherit security policies from its parent.
- ☐ The owner has full control over the resource.
- ☐ Administrators with the Manage Private Resources privilege over a group to which the owner belongs can take control of the resource. This allows administrators to manage resources belonging to inactive or deleted users, whether by deleting the resources, publishing them, or transferring their ownership to another user or group.
- ☐ A private resource may be owned by a group or a user, but it may not have multiple simultaneous owners. For a group to own a private resource, an authorized user, such as an owner or an administrator with the appropriate privileges, must transfer the ownership from a user to the group.
- ☐ ReportCaster schedules can only be owned by a user.

Private content comes in the following forms:

#### *My Content*

The reports, output, and schedules created by a user. This content remains private to a user unless the user is authorized to share it with others and chooses to do so, or unless an administrative user with the ability to manage private content for that user publishes the content.

#### *Other private content*

Private content that is intended to be accessed by a particular group of developers or that is being prepared for publication. This allows new content to be tested before publication even when it is created in a production environment, a situation most typical of SaaS deployments, where tenant developers may only have access to a single environment.

A My Content folder can be created automatically for published folders to give users a place to save items, such as procedures and reports. The parent folder must have the Automatically Create a My Content Folder property enabled and the user must have the My Content Folder privilege.

The Automatically Create a My Content Folder property is activated, by default, for top-level folders created from the Enterprise Domain Resource Template. It is not activated, by default, for top-level folders that are not based on the Enterprise Domain Resource Template. To add a My Content folder to these folders, follow the steps in the topic, [How to Add a My Content Folder](#) on page 359.

**Note:** We recommend that you set this property only on top-level folders.

### **Procedure:** How to Add a My Content Folder

1. Right-click the folder, and select *Properties*.
2. In the Properties panel, select the *Advanced* tab.
3. Select the *Automatically create My Content folders* check box, and then select *Save*.
  - ☐ If the folder is published, the screen refreshes, the cursor moves to the parent folder or workspace, and a My Content folder is created. To see it, expand the folder you just updated.
  - ☐ If the folder is not published, a My Content folder is created when you later publish the folder.

**Note:** If you clear this check box after creating a My Content folder, the My Content folder is not removed.

### *Published Resources*

Authorized users can publish private resources to make authoritative content available to a larger set of users. The security policy for published resources specifies the following conditions:

- ☐ Published resources are owned by the system.
- ☐ A published resource is subject to the security policy defined on its parent folder.

### *Shared Resources*

Sharing is a feature that is generally used to enable users to share private content residing in their My Content folders with authorized colleagues.

Shared resources are made available to other appropriate users through a special Shared Content folder. The Shared Content folder is a virtual folder that appears automatically in a folder whenever there is shared content inside that folder.

The Content Sharing Scope privilege determines the users and groups with whom the owner is authorized to share resources. The content owner must also be permitted one or more of the following privileges located under the Advanced Reporting folder of the Role dialog box.

### Share Private Resources

The user can share resources by selecting *Share* from the resource shortcut menu. A resource is shared with everyone who can access the folder that contains it. This does not apply to library content.

### Share Private Resources with Specific Users

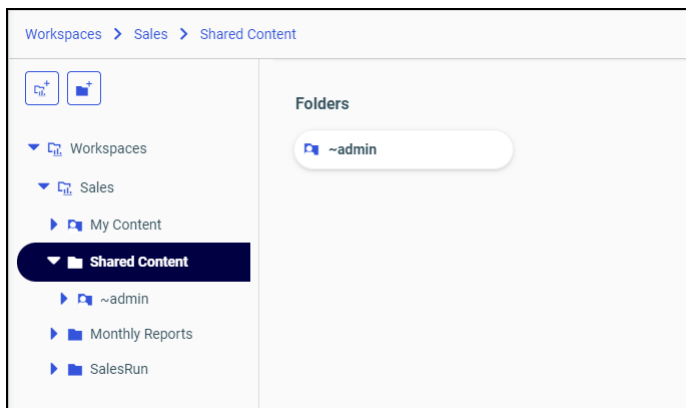
The user can share resources by selecting *Share with* from the resource shortcut menu and clicking from a list of authorized users, groups, or users and groups. This does not apply to library content.

### Share Private Library Content

The user can share library content.

There are two ways to share private resources from your My Content folder or folders within it. You can use the Share menu option to share a resource with everyone automatically, or you can use the Share With menu option and share the resource with a limited set of users or groups selected from the Share With dialog box. When you use the Share option, you share the resource with the EVERYONE group and grant basic user privileges to all users. When you use the Share With option, you share the resource with a limited number of selected users and groups, and grant privileges to them based on their role in the workspace in which the resource appears. You can use the Share option to make a resource generally available while it is still in development, and use the Share With option to share resource development tasks with other users without making the resource generally available.

When you share a resource from your My Content folder or one of the folders within it, all users other than yourself will see it under a folder entitled Shared Content. When you open a Shared Content folder, you see a subfolder for each user who has shared content with you. This feature helps you distinguish between content you created, which appears in the My Content folder, and content created by others but shared with you. In the following image, the Administrator folder, which contains content the Administrator made available to an individual user, appears under the Shared Content folder as shown in the Content view.



### Understanding How Sharing Affects Folders and Resources in the Hierarchy

In order to protect the integrity of unshared resources within a workspace while continuing to grant appropriate access to shared resources, the folders and parent folders that contain a resource adjust their own shared status automatically.

When you share a resource within a folder, that folder and all of its parent folders up to the My Content folder, are shared automatically. This automatic update helps ensure that a newly-shared resource will not be unavailable because it is located in a folder that is not shared. The same behavior occurs if you share a folder within a hierarchy. All folders above the shared folder, up to the My Content folder, are shared automatically. This behavior automatically ensures that no unshared folder in a hierarchy will block access to shared folders or resources under it.

If you unshare a folder after sharing it, the shared resources within it are also unshared automatically in keeping with the unshared status of the folder in which they appear. The same behavior occurs if you unshare a parent folder in a hierarchy. All folders and resources under the newly unshared folder are also unshared automatically. This behavior ensures that all folders and resources within an unshared folder are rendered unavailable and reinforces the decision to make a folder and the resources within it unavailable to other users.

If you share a folder again after unsharing it, the resources within it are not shared automatically. You must open the folder and share the resources within it individually. The same behavior occurs if you share a parent folder in a hierarchy after unsharing it. None of the folders and resources under the re-shared folder are shared again automatically. You must open and share them individually, but remember that sharing a resource within a hierarchy automatically shares the folder and any parent folders that contain it. This behavior enables you to maintain shared and unshared resources in the same folder, and keeps unshared resources unavailable even though they are located within a shared folder.

When you unshare an individual resource within a shared folder, you do not automatically unshare the folder in which it appears. That folder continues to be shared until you unshare the folder itself. This feature ensures that a folder continues to provide access to shared resources even though one or more resources within it are no longer shared. The same behavior occurs if you unshare a folder within a hierarchy, the folders above it remain shared until you change the shared status of those folders individually.

As a rule, sharing a resource or folder automatically shares the folders above it. Unsharing a folder automatically unshares the folders and resources below it. The only exception to this rule are individual resources or folders that have no folders under them. When you unshare these items, there is no impact anywhere else in the hierarchy.

Once you share an individual resource, that resource remains shared until you unshare it or until you unshare the folder or parent folder that contains it. Once you share a folder, it remains shared until you unshare it or a parent folder. You can unshare an individual resource without unsharing the folders that contain it. This behavior keeps shared resources available even if they are included in a folder with unshared resources.

### Sharing Resources

The ability to share or unshare private resources only applies to resources located in the My Content folder of a workspace or in one of the child folders within the My Content folder. For more information about how to share resources, see the *Configuring and Using Your TIBCO WebFOCUS® Environment* technical content.

### Rules

Rules determine what a user is allowed or not allowed to do in any particular location. A rule associates a resource with a subject (a user or group), a role, an action (such as permit or deny), and a scope (whether the rule applies only to the resource, only to its contents, or to both). Through these rules, users are either permitted or denied the various privileges contained in the role.

**Note:** Typically, the subject of a rule is a group. It is possible to apply a rule to a single user, but it is not recommended, because managing the rules on an individual user basis can become unwieldy.

### Effective Policy

A combination of rules determines whether or not a user can access a particular tool, resource, or ability. Users who belong to multiple groups may be permitted the use of a tool in one group and denied the use of the tool in another. A folder may have no rules explicitly applied to it, but inherit the rules of its parent folder. When a user attempts to access a resource, all of the relevant security rules are evaluated, and the result of the combined rules for the user on that resource is determined. This result is the effective policy for the user on the resource.

Rules that are relevant to the given subject and resource can include:

- ☐ Rules that apply to the resource for the explicit and implicit groups to which the user belongs.
- ☐ Rules that apply to the resource directly for the user account.
- ☐ Inherited rules that apply to the parent of the resource for the user or group.

When a user does not have the abilities that you expect, reviewing the effective policy for users can be a helpful troubleshooting step.

### Order of Precedence

Conflicts between rules are resolved by the order of precedence. Listed in descending order, the order of precedence is:

- ☐ Clear Inheritance
- ☐ Over Permitted
- ☐ Denied
- ☐ Permitted
- ☐ Not Set

In general, rules are used to permit privileges, because, by default, privileges are not permitted. Privileges not explicitly permitted (by Permit or Over Permit) are denied. By default, privileges are Not Set, which means they are not permitted. When one rule permits a privilege for a user on a resource and another denies it, the privilege is typically denied. (Session privileges are treated differently, as discussed below.) Permitted rules overturn Not Set rules, resulting in an effective policy that permits the privilege. Denied rules overturn Permitted rules (except for session privileges), resulting in an effective policy that denies the privilege. Over Permitted rules overturn Denied rules, resulting in an effective policy that permits the privilege.

No group takes precedence over another group and user rules do not take precedence over group rules. If you would like to permit individual users a privilege denied to their groups, you cannot permit this privilege simply by creating a rule that permits the privilege for the user on the selected resource, because the effective policy for the user is determined by prioritizing the rule that denies the privilege to the group over the rule that permits the privilege to the user. Instead, you must create a rule that over permits the privilege to the user, which will be prioritized above the rule that denies the privilege to the group.

Over Permitted rules are typically used to address unusual situations, such as when one member of a group needs access to a resource, but access is denied to that group. Over Permitted rules can also be used to ensure that a privilege is always permitted to a particular group, no matter what other rules apply. For example, a built-in rule that Over Permits the Full Control role to members of the Administrators group on IBFS:/ (the entire file system), with the scope of folder and children is included. This rule is a safeguard that prevents administrators from losing control of resources within the system if a Denied rule is applied to the EVERYONE group.

The Clear Inheritance rule removes an inherited rule for a role on a resource, changing the access on the resource to Not Set. When a user belongs to multiple roles with overlapping privileges, any privileges shared with the cleared role are evaluated to Not Set.

Session privileges enable menu bar drop-down list items, nodes on the Resources tree, and other global user capabilities, such as many of the buttons in the desktop products. Because session privileges govern access to tools that may be necessary in multiple locations, a session privilege is permitted when it is denied by one rule but permitted by another. For example, if you are able to run deferred procedures in the Sales folder but denied this ability in the Finance folder, you still need access to the Deferred Status interface so that you can see your deferred reports from the Sales folder.



### Procedure: How to View the Effective Policy for a User on a Resource

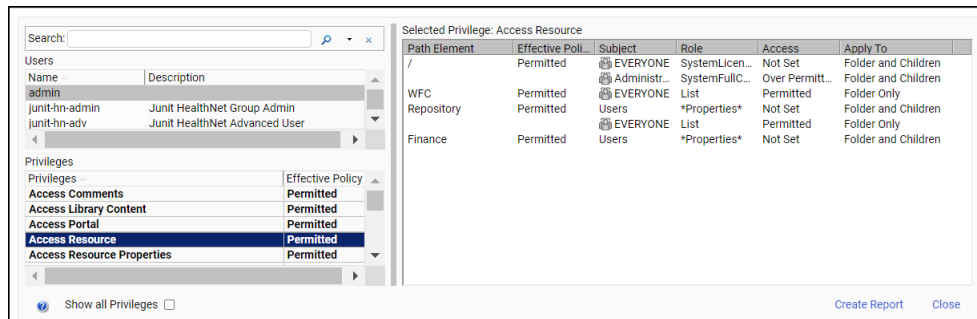
The Effective Policy dialog box indicates why a user does or does not have a certain capability. To view the effective policy of other users, you must be permitted the following privileges:

- ☐ View Rules on a Resource (opViewRulesOn), which enables the *Rules on this Resource* and *Effective Policy* options on the Security shortcut menu.
- ☐ Manage Rules on Resources (opManageRulesOn), which enables the *Rules* option on the Security shortcut menu.

Users with only the View Rules on a Resource privilege may view the effective policy only for themselves, on particular resources. If a user does not have the appropriate privileges, the options to view or manage rules and effective policy will not appear in the shortcut menus.

1. Right-click a resource and click *Security*, then *Effective Policy*.

The Effective Policy dialog box appears, listing the effective policy calculated for each privilege appearing in a rule on this resource.



If you have the appropriate privileges, you can select other users from the User drop-down list to see their effective policies.

2. To show the effective policy for all privileges for this user on this resource, including those not applied to the resource in any rules, select *Show all Privileges*.
3. To see how the effective policy for a privilege is evaluated, select the privilege in the Privileges box.

The Effective Policy dialog box displays the policy evaluation for all the groups to which the user belongs at every level of the hierarchy above the resource, displaying the following information for each level:

- ☐ Path Element.
- ☐ Effective Policy. The access set on this folder by the combination of all applicable rules.

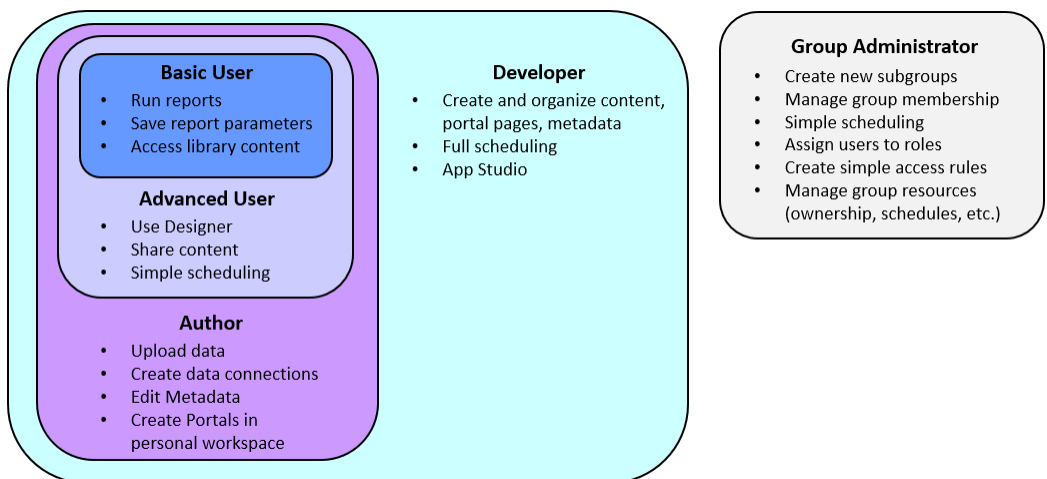
- ☐ Subject.
  - ☐ Role.
  - ☐ Access. The access set on this folder by rules applying directly to this level of the hierarchy.
  - ☐ Apply To. Whether the policy applies to the folder for the path element only, the folder and its children, or only the children of the folder for the path element.
4. To produce a rich text version of the information produced in the dialog box, select a privilege and click *Create Report*.

## Policy Design

A security policy controls access to reporting resources according to your business needs. When you design a policy, you determine which groups, roles, and rules to create.

## Group Design

The resource templates define four roles (Basic User, Advanced User, Developer, and Group Administrator), which are implemented as nested subgroups underneath a parent group for the workspace. The capabilities of users in the Basic User group are determined by rules associated with the Basic User role, while the capabilities of users in the Advanced User group are determined both by rules associated with the Basic User role and by rules associated with the Advanced User role. The Advanced User capabilities include those possessed by Basic Users, and Developer capabilities include those possessed by Advanced Users, as shown in the following diagram. Group Administrators are not allowed to run reports or view library output, so their capabilities do not overlap with those of the other subgroups.



Nesting roles simplifies policy design. A user only needs to belong to one of these groups to have the full capabilities of that type of user. A user can also be added to the Group Administrator groups and one of the other groups, if there is a requirement for an individual to have this blended set of capabilities. Rules can be applied to a parent group to allow all its users to share content with each other, or to give group administrators control over that parent and its subgroups.

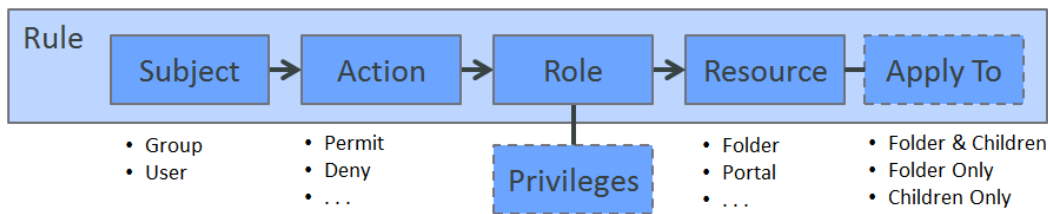
Alternatively, you can partition user capabilities into distinct roles with no overlapping privileges. While this model affords the most flexibility, it is also more difficult to administer because the capabilities of each user are a composite of many roles and rules.

In addition, you may need infrastructure groups to organize users who require access to all resources in the system. For example, an Administrators group, or a Change Control group that has the authority to export resources across the Repository, but is not able to run or delete resources.

For more information about groups, see [Managing Users](#) on page 444.

## Role Design

Roles are used to bundle a set of privileges commonly used together. A security rule then permits or denies the role for a subject to a resource, as shown in the following image.



Once you have determined how to organize users into groups, you can design roles that will be useful for these groups. If there is one group per user type, as there is in the resource templates, a simple way to begin is to create one role per user type. You can then create rules which permit or deny each role to its respective group for a particular resource.

For example, the resource templates already create a rule that permits the BasicUser group the DomainBasicUser role on the workspace folder and its children. The AdvancedUser group is permitted the DomainAdvancedUser role on the workspace folder and its children. You can design similar rules to provide the custom subgroups that you create with the appropriate access to a workspace portal, or to a workspace page on a common portal. To ensure developer access to the Reporting Server, you can create a rule granting the Developer group the DomainDeveloper role on the Reporting Server node in the Resources tree.

One role can be used in multiple rules, such as when you would like to permit privileges to a group on different types of resources. If you would like to grant developers privileges on a folder, a portal, and a Reporting Server node, you can create one role which collects all the relevant privileges, and then create a separate rule to apply the role to each resource. Privileges that do not apply to a given subsystem are ignored. You can also create a separate role for developers on each resource, which collects only the privileges relevant to the associated IBFS subsystem. You would create a role for developers that specifies the folder, a role for developers that specifies the portal, and a role for developers that specifies the Reporting Server node. However, a single role is easier to maintain.

**Note:** Roles that include session privileges should not be used in rules that are set in the lower branches of the WFC subsystem. By default, session privileges below a certain depth are not checked, in order to decrease the demand on system resources. The search depth can be changed by a system administrator, but it is not recommended.

For more information about roles, see [Managing Roles](#) on page 463.

## Rule Design

The fewer rules a system has, the easier it is to understand and maintain. The number of rules comprising your security policy depends on many factors, such as which subsystems you want to expose to users, how many different roles your organization requires, and how many workspaces you have. You can minimize the number of rules in your system by applying the rules to the highest possible level in the IBFS hierarchy. In general, this means permitting privileges at the highest possible level, then denying them at lower levels, as needed.

As an example, consider a simple scenario where everyone in an installation has access to all its resources and end users only need to do one of two things: develop reports or run them. You can implement this simply by using two groups and two rules. The two groups are the Report Developer group and the Report Runner group. The two rules are placed on the IBFS root node, and therefore, apply to all content folders, portals, and Reporting Server resources. One rule permits the Report Developer group the Report Developer role on the IBFS root folder and all its children, and the other rule permits the Report Runner group the Report Runner role with the same scope. With a single additional rule, you can hide the Reporting Server node from the Report Runner group by denying the group the List role on that node.

Frequently, different groups require access to different resources. The security policy provided by the resource templates supports this requirement. In each workspace, groups are granted access to their own resources, and no groups are associated with the rules above the workspace folders and portals. Specialized rules can be applied to adjust the policy to support additional needs, such as hiding specific folders or portal pages.

One common requirement is that users need to be able to act on the contents of a container, but should not be able to affect the container itself. For example, developers may need to create and delete folders under Sales, but should not be able to delete the Sales folder itself. You can ensure this by restricting specific privileges with a rule that is used on the folder only. The resource templates restrict Workspace Developers and Group Administrators in this way, so they do not delete the containers that define their security boundaries, such as the folders over which they have administrative control.

For more information about rules, see [Managing Rules](#) on page 470.

## Working With Folders

Folders contain all repository content. Whenever a user creates a folder, it will always be created as a private folder. If the creator is permitted the necessary privileges, folders and their contents can be shared with other users or published for general use.

Folders have both titles and names. The title of a folder is typically displayed to users, and WebFOCUS uses the folder name as an internal reference to provide an unambiguous context for the content it contains. Titles can be duplicated within a container, but folder names cannot.

A folder path may have up to 1,040 characters for path information, excluding the object name, and up to 64 characters for the object name. For example, a folder may be named: /WFC/Repository/AmericaBank/Finance. In this example the path information, /WFC/Repository/AmericaBank/, is 28 characters, and the folder name, Finance, is 7 characters.

**Note:** In versions prior to WebFOCUS 8, published content is known as Standard Reports, and private content is known as My Reports.

### **Procedure:** How to View Folder Properties

In order to view the properties of a folder, right-click a folder in the Resources tree or content area, and then select *Properties*. The Properties panel appears, displaying the information in the following table.

Item	Description
<b>General Tab</b>	
Title	Displays the title that appears on the folder when it is displayed in the Resources tree or content area. This is the title by which end users identify the folder and is typically based on the contents in the folder.

Item	Description
Name	Displays a unique internal reference to the folder. This is the name used to identify the folder for internal operations. This field is dimmed and unavailable by default. Click the <i>Change Name</i> icon next to it to make this field available for name changes.
Summary	Displays a detailed explanation that provides additional information about the folder.
Path	Displays the full repository path of the parent folder.
Created	Displays the date and time the folder was created and the ID of the user who created the folder.
Modified	Displays the date and time the folder was last modified and the ID of the user who last modified the folder.
Accessed	Displays the date and time the folder was last accessed by the Properties, Run, or Run Deferred commands, or by any of the edit tools used to update the folder. It also displays the ID of the user or tool that last accessed the folder.
Owner	Displays the ID of the User to whom the folder is currently assigned.
Publish	Specifies whether the folder and its contents are published or not.
Show	Specifies whether to display the folder to users who are not permitted to create content in the folder. This option is primarily used when the folder needs to be made temporarily unavailable to end users who would otherwise be permitted to view or work with the content in the folder.

#### Advanced Tab

#### Folder Properties

Automatically Create My Content Folders	When this check box is selected, a My Content folder is created for users with the My Content Folder privilege, giving them a place to save the personal reports, charts, or documents that they may create using WebFOCUS Designer, InfoAssist, or other report and distribution features, such as Save Parameter reports.
---	---

Item	Description
Automatically Open	<p>If this check box is selected, when you open the Workspaces view from the Hub, the WebFOCUS Home Page, or the Legacy Home Page and load the Resources tree:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> The folder for this workspace on the Resources tree expands automatically and displays the My Content folder and other folders within it.</li> <li><input type="checkbox"/> In the Hub Workspaces view, or on the WebFOCUS Home Page, the content area also automatically opens the folder for this workspace and displays the folders and items assigned to it.</li> </ul>
<b>Explorer/Portal Properties Group</b>	
Sort order	Specifies the order in which the folder is listed in the Resources tree and in the content area.
Language	Displays the language in which the folder and its content were created.
View All	Opens the Language Properties dialog box that displays the default language in which the folder and its contents were created and are displayed. If your environment supports multiple languages, this dialog box also contains entries for any additional languages made available by your code page selection.
Menu Icon	Contains the CSS class name of the icon that is used to represent this folder in the tabs above the full sized home page display or on the side menu when the display is less than full size. For more information see the <i>Adding Icons to Portal Levels</i> topic in the <i>Building Portals</i> technical content.
Show menu icons for children	When this check box is selected, folders and portals within this folder can display a menu icon in the tabs above the full-sized home page display or on the side menu when the display is less than full size.
<b>Server Tab</b>	

Item	Description
Assign Server	<p>Displays the assigned server and all available servers. When this check box is selected, the default WebFOCUS Reporting Server is not in use, and one of the available servers must also be selected.</p> <p>When this check box is cleared, a WebFOCUS Reporting Server is not specified, and the report request is submitted to the default WebFOCUS Reporting Server that is specified in the WebFOCUS Client configuration.</p>
Assign Application Path	<p>Displays the assigned Application Path and all available Application Paths. When this check box is selected, the default Application Path is not in use, and one of the other available Application Paths must also be selected.</p> <p>When this check box is cleared, an Application Path is not specified, and the default Application Path defined during the processing of the WebFOCUS Client configuration and the WebFOCUS Reporting Server configuration is used.</p>

**Procedure: How to Create a Folder**

1. In the Resources tree, navigate to the workspace or folder that will contain the new folder.  
Or  
In the breadcrumbs trail, click the link to the workspace or folder that will contain the new folder.
2. In the Hub, select *New Folder* above the Resources tree.  
Or  
On the WebFOCUS Home Page, in the Action Bar, select the *Other* tab, and then click *Folder*.



3. In the New Folder dialog box, type the title for the new folder, as shown in the following image.

The image shows a 'New Folder' dialog box. It has a title bar with the text 'New Folder' and a close button (X). Inside the dialog, there are two text input fields. The first field is labeled 'Title' and contains the text 'Region One-Sales'. The second field is labeled 'Name' and contains the text 'Region\_One-Sales'. At the bottom right of the dialog, there are two buttons: 'Cancel' and 'OK'.

As you type, a unique value derived from the value in the Title field is simultaneously typed in the Name field. Any spaces or special characters you type in the Title field are automatically converted into underscore characters in the Name field. If you type an unbroken string of multiple special characters, such as &&&, in the Title field, the Name field automatically converts them into a single underscore character. If you prefer, you can modify the Name later.

4. Click **OK**.

The new folder appears in your selected location in the Resources tree and in the content area.

5. Perform the following substeps to add an optional summary description of the folder:
  - a. Right-click the new folder, and then click *Properties*.
  - b. In the Properties panel, type the description in the Summary field.
  - c. Click **Save** to save the description, and then click *Cancel* to close the Properties panel.

### **Procedure: How to Publish a Folder**

In the Resources tree or content area, right-click a folder, and then click *Publish*.

The Resources tree refreshes and no longer displays the folder name in italics. The content area refreshes, removes the border from the folder, and displays the folder icon in full color.

### **Procedure: How to Unpublish a Folder**

In the Resources tree or content area, right-click a folder, and then click *Unpublish*.

The Resources tree refreshes and displays the folder name in italics. The content area refreshes, displays a border around the folder, and displays the folder icon in gray.

**Procedure: How to Duplicate a Folder**

In the Resources tree or content area, right-click a folder and then click *Duplicate*.

In the Resources tree, a duplicate folder appears beneath the original folder. In the content area, the duplicate folder appears immediately to the right of the original or below it. The name and title of the duplicate folder are the same as those of the original, appended with an underscore and an integer that increases each time the folder is duplicated.

**Notes:**

- ☐ The *Duplicate* menu option creates a copy of the folder in the same location as the original. Use the *Copy* and *Paste* options if you need to move a copy of a folder to a different location.
- ☐ You cannot duplicate a workspace.

**Procedure: How to Cut or Copy and Paste a Folder**

1. In the Resources tree or content area, right-click a folder, and then click *Cut* if you want to move the folder, or click *Copy* if you want to move a copy of the folder and leave the original folder in place.
2. In the Resources tree, click the folder that represents the new location. Expand the tree to display the new location if necessary.

or

If the new location appears on the breadcrumb trail, click the folder that represents the new location.

3. In the Resources tree, right-click the folder that represents the new location, and then click *Paste*.

or

Right-click anywhere in the content area of the new location, and then click *Paste*.

The Resources tree and the content area refresh and display the folder.

Folder names must be unique within a specific location. If you paste the folder to a different parent folder, its name remains the same, as long as no folder of that name already exists in the new parent. If a folder of that name already exists, or if you pasted the copy of the folder into the same folder as the original, the name of the copy is the same as the original, appended with an underscore and an integer that increases each time you paste the folder. Folder titles are updated in the same way as folder names.

**Note:** You cannot cut and paste a workspace.

**Procedure: How to Change a Folder Title**

1. In the Resources tree or content area, right-click a folder, and then click *Properties*.
2. In the Properties panel, type the new Title in the Title field, and then click *Save*.

The folder name is updated. If the new name changes the position of the folder in alphabetical order, the folder is also relocated on the Resources tree and within the content area.

3. When your updates are complete, click *Cancel* to close the Properties panel.

**Procedure: How to Delete a Folder**

1. In the Resources tree or content area, right-click a folder, and then click *Delete*.
2. When you receive a message asking you to confirm the decision to delete the folder, click *OK*.

The Resources tree and the content area refresh and remove the deleted folder.

## Understanding Workspaces

Workspaces are a basic building block of WebFOCUS content organization. Each workspace combines a collection of user groups, a link to the metadata on which content in the workspace is based, and a set of rules that makes them all work together. Workspaces enable users to maintain private content, to share that content if their user role permits, and to access governed content published by others.

In the Resources tree, workspaces appear as root-level folders under the Workspaces node. These folders partition content into sections that users can easily identify, and create an organized content structure for a workgroup.

There are two types of workspaces, Enterprise and Tenant. Enterprise workspaces support installations that affect a single enterprise and are organized by department and content within that enterprise. Tenant workspaces support installations that affect multiple enterprises and are organized by tenant clients of a software as a service vendor.

Tenant workspaces are available only to the users assigned to the tenant. They are not available to users assigned to any other tenant.

Resources, such as Portals, Shared Portal Pages, or WebFOCUS Reporting Server Templates, are also part of workspaces. To create these resources, you must first create a workspace. Workspaces link the content used by these resources to the users to which they will be made available. The rules defined within workspaces govern the access of users to the content in each resource. When these resources are no longer needed, they are deleted by deleting the workspace to which they are assigned.

By default, resource templates are used as the basis for all new workspaces. When you create a new workspace, the resource template that corresponds to the type of workspace you select and the resources you want to include with it is invoked. The preconfigured groups and rules within a resource template define a range of availability from the broadest level of access to the most restricted level. WebFOCUS defines a basic set of templates, but administrators can create their own resource templates and add them to the list of available resource templates.

### Understanding My Workspace

My Workspace is a specialized workspace that gives users a readily-accessible location where they can create content for their own use and share it with others. It is included, by default, in a product installation, and it is designated, by default, to be the workspace in which content created directly from the Home Page or outside of any other named workspace is stored.

Like other workspaces, My Workspace is created from the resource template and uses the same security rules assigned to all templates. However, instead of the four groups that are typically assigned to workspaces, it contains only the Basic Users group and the Authors group.

As with any other workspace, administrators must actively manage the assignment of users to the two groups within My Workspace. Privileges granted to a user in My Workspace are entirely independent of privileges granted to a user in any other workspace.

The My Content folder in My Workspace serves as the dedicated location in which members of the Authors group can create new content. The Shared folder is also included and becomes visible when users share private content within their own instance of My Workspace.

Note that the *workspace* entitled My Workspace is distinct from the *view* entitled My Workspace. Both the view and the workspace contain private content created by the user who is currently signed in.

However, the workspace only contains content created in or saved to it by the user who is currently signed in. The view displays private content from the My Content folders of all of the workspaces available to that user. The My Workspace view, therefore, contains a broader range of content than the workspace entitled My Workspace.

If it is necessary to use a different workspace as the default workspace for new content, administrators can replace My Workspace with another workspace by updating the path that appears in the Default Workspace Repository Path (IBI\_DEFAULT\_WORKSPACE\_PATH) setting on the BI Portals page.

However, even when another workspace is defined as the default workspace, users can still work within the workspace entitled My Workspace by opening it from the Hub or the WebFOCUS Home Page content view.

## Understanding the Getting Started Workspace

The Getting Started workspace is a specialized workspace that contains content displayed in the Getting Started carousel that can appear at the top of the Workspaces view from the Hub, or the WebFOCUS Home Page in the Cloud instance of the product. When you first install the product, this workspace contains content that is designed to introduce new users to the capabilities of WebFOCUS software. Administrators can add their own customized content to this workspace in order to tailor the introductory content to the needs of their organization. Depending on the privileges of the Getting Started workspace group to which they are assigned, individual users can run, edit, create, or schedule items within this workspace and its associated carousel.

The Getting Started workspace is included, by default, in the Cloud instance of the product, but is not included in the On Prem instance. Like other workspaces, it is created from the resource template and uses the same security rules assigned to all templates.

The Getting Started workspace includes the four user groups that are typically assigned to workspaces, and adds the Authors group. The inclusion of all five groups created by the resource template allows administrators to assign new users to the complete range of capabilities that most closely matches the role they will typically play.

As with any other workspace, administrators must actively manage the assignment of users to groups within the Getting Started workspace. Privileges granted to a user in the Getting Started workspace are entirely independent of privileges granted to that user in any other workspace.

The folders provided, by default, with the Getting Started workspace also differ from other workspaces created from the resource template. The Getting Started workspace does not display a My Content folder. However, it does display a Visualizations folder. This folder contains pre-packaged visualizations that are not displayed in the Getting Started carousel, but are available to users as examples of WebFOCUS content.

Administrators can replace the Getting Started workspace with a different workspace by changing the value assigned to the Default List Repository Path (IBI\_DYNAMIC\_LIST\_PATH) setting on the BI Portals settings page, located on the Configuration tab of the Administration Console. This setting also determines the workspace that appears in the top level carousel on the Home View of the WebFOCUS Home Page.

When an administrator replaces the default path to the Getting Started workspace in this setting, the name of the top carousel is replaced with the name of the different workspace and the content contained in that workspace appears in the carousel. Administrators must assign users to the groups within that workspace in order to make the content displayed in the top level carousel available to them. Note that the Authors group is absent from any other workspace that would replace the Getting Started workspace.

If the value in this setting is blank, the Getting Started carousel does not appear at the top of the Home View, but the Getting Started workspace and its group assignments remain in place.

Even when a different workspace, or no workspace at all, is identified in this setting, users can still work within the workspace entitled Getting Started from the WebFOCUS Home Page content view.

## Understanding Resource Templates

The WebFOCUS security model offers administrators the flexibility to establish complex security policies. However, many organizations find that their security needs can be met by a small number of standard user roles and a straightforward pattern of access rights. WebFOCUS provides resource templates for enterprises with departments or divisions, and SaaS providers who require both common and tenant-specific reporting resources when creating workspaces.

WebFOCUS provides several resource templates that will create folders, groups, roles, and rules for typical enterprise or SaaS deployments. You can implement the templates as is, or adapt them to your requirements. You can also develop custom resource templates for your organization.

## Understanding Resource Template Groups

When you create a new workspace from a resource template, a new group is automatically created for the workspace itself, along with subgroups for each of the following four user types within it: Basic User, Advanced User, Developer, and Group Administrator. When Administrators assign users to one of these groups, they automatically give those users the privileges assigned to the user role when working with that workspace.

Members of the Basic User group can view content within their workspace. They can create folders within the My Content folder and save deferred reports to them. They can also copy autolink parameters from a previously created report and save them in their folders. They cannot share, publish, copy, or paste any folder or content.

Members of the Advanced User group have all of the privileges of Basic Users, and they can create and share their own content and folders.

Members of the Developers group have all of the privileges of Basic and Advanced Users, and they can upload and connect to data, edit metadata, and create and organize workspace content. They can manage content made visible to other users. They can also copy and paste folders and content from their workspace to another workspace, but they must be sure that the workspace they target for this operation maintains connections to the same metadata as that used to create the content they are copying.

Members of the Group Admin group determine the role each user can have within a workspace by adding users to or removing users from one of the four user type groups and can change the General Access setting assigned to the workspace.

These four user types cover the basic access levels that the majority of users will require when working with workspaces, freeing administrators to focus on the assignment of users to these four groups instead of requiring them to configure access level profiles for each user.

### ***Procedure:*** How to Create a Workspace

1. Sign in as an administrator, and on the Hub, select the Workspaces icon from the side navigation pane to open the Workspaces area.

Or

Open the WebFOCUS Home Page and on the Banner, select *Workspaces*, to open the Workspaces area.

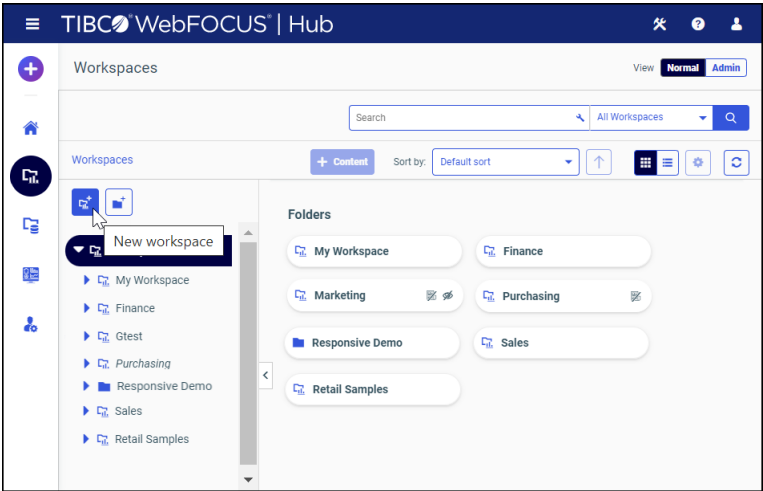
**Note:** Expand the Resources tree, on the left of the content area, if it is not open by default.

2. In the Resources tree, select *Workspaces* if it is not highlighted already.

Or

In the breadcrumb trail, select *Workspaces*.

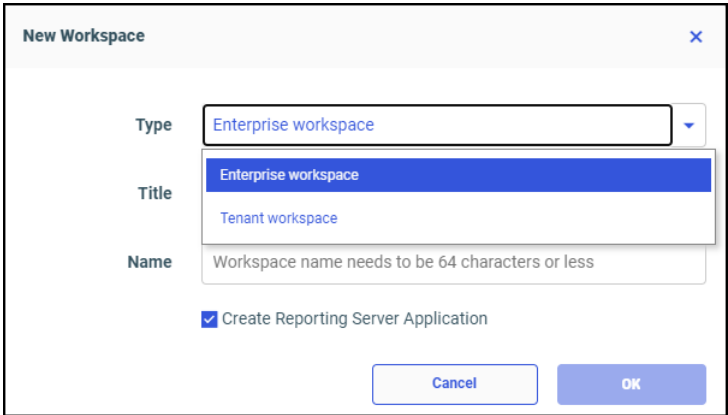
- 3. In the Hub, select *New workspace* above the Resources tree, as shown in the following image.



Or

On the WebFOCUS Home Page, open the Workspaces view, and in the Action Bar, under Create New, click *Workspace*.

- 4. In the New Workspace dialog box Type list:
  - Click *Enterprise workspace* to create a department or division workspace for an enterprise, as shown in the following image.



- Click *Tenant Workspace* to create a tenant workspace for a SaaS provider.



5. In the Title field, type a description of the workspace, as shown in the following image.

The screenshot shows a 'New Workspace' dialog box with the following fields and options:

- Type:** A dropdown menu with 'Enterprise workspace' selected.
- Title:** A text input field containing 'Human Resources'.
- Name:** A text input field containing 'Human\_Resources'.
- Checkboxes:** A checkbox labeled 'Create Reporting Server Application' is checked.
- Buttons:** 'Cancel' and 'OK' buttons are located at the bottom right.

As you type, the description you type in the Title field, adjusted to conform to IBFS rules, is automatically assigned to the Name field.

Administrators can localize the title for different languages by opening the Properties panel after the workspace is created and adding localized titles for the languages on display in the Language Properties dialog box linked to the Properties panel by the View All button.

6. To create an associated application directory on the WebFOCUS Reporting Server, select the *Create Reporting Server Application* check box.

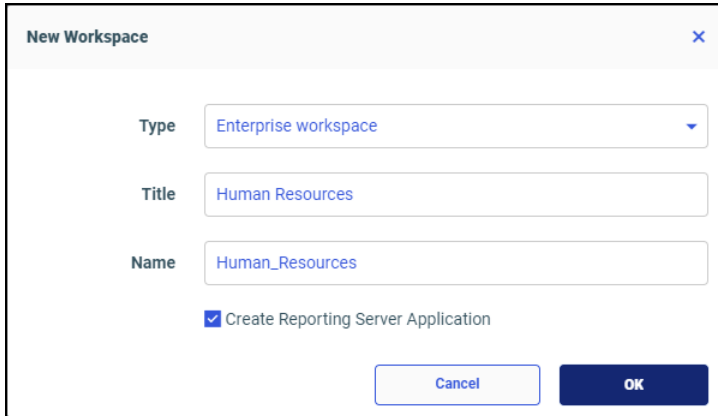
**Note:** If you include the Create Reporting Server Application option, you need to create and implement an authorization strategy that grants workspace users appropriate access to application directories on the WebFOCUS Reporting Server. For more information, see [Understanding Access Control Templates](#) on page 401.

As you select or clear this check box, the value in the Name field is updated dynamically to remove characters that are not allowed for resource names.

7. When your selections are complete, click *OK*.

## Naming a New Workspace

When you type the description of a new workspace in the Title field of the New Workspace dialog box, the same characters are typed automatically in the Name field. The Name field description is automatically validated for compliance with IBFS naming rules. If you type a restricted character into the Title field, the Name field substitutes the restricted character with one that is permitted. For example, if you type a space in the Title field, the Name field will replace it automatically with an underscore (\_) character, as shown in the following image.



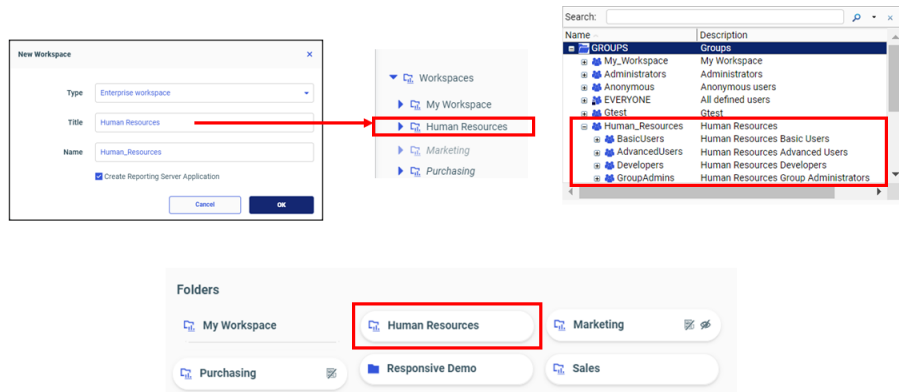
The screenshot shows a 'New Workspace' dialog box with a close button (X) in the top right corner. It contains three input fields: 'Type' (a dropdown menu showing 'Enterprise workspace'), 'Title' (a text box containing 'Human Resources'), and 'Name' (a text box containing 'Human\_Resources'). Below these fields is a checked checkbox labeled 'Create Reporting Server Application'. At the bottom right are two buttons: 'Cancel' and 'OK'.

The value in the Title field is displayed to end users automatically, and the value in the Name field is used for internal operations.

## Viewing the Results of a New Workspace

When you create a new workspace, the results appear in the Workspaces view and in the Security Center. Required resources are created based on your selection.

When you create a workspace from the Workspaces area, a folder for the new workspace is displayed on the Resources tree and in the Folders section of the content area. In the Security Center, a group for the new workspace appears in the Groups pane of the Users and Groups tab. The Resources tree and the content area show Titles, by default. Groups listed in the Security Center show both the Name and the Title of the workspace simultaneously. The results are visible in the Workspaces area and in the Security Center, as shown in the following image.



When creating a workspace from the Workspaces area of the Hub or WebFOCUS Home Page, there is no option to create a portal or shared portal page along with the workspace, so these results are not visible. However, if you create a workspace from the Legacy Home Page, you do have the option to include a portal or shared portal page in the process.

If you select the Workspace Portal option from the Legacy Home Page version of the New Workspace dialog box, the portal becomes available along with the other results. A folder for the new workspace appears on the Resources tree and in the Folders section of the content area. An icon for the portal also appears in the Portals carousel. In the Security Center, a group for the new workspace appears in the Groups pane of the Users and Groups tab. The Resources tree, content area, and Portals carousel show Titles, by default. Groups listed in the Security Center show both the Name and the Title of the workspace simultaneously. These results are visible in the Workspaces area, in the Portal carousel, and in the Security Center.

If you select the Workspace Page in a Shared Portal option, the shared portal page becomes available along with the other results. This option creates an empty Fluid Canvas page in a shared portal. In the Shared Enterprise Portal itself, a folder for the shared page appears in the Resources tree. These results are visible on the WebFOCUS Home Page.

## Understanding Differences Between Enterprise Resource Templates and Tenant Resource Templates

Each resource template creates multiple groups, roles, security rules, and folders, and, if selected, portals, portal pages, or WebFOCUS Reporting Server applications. However, there are several differences between an Enterprise Resource template and a Tenant Resource template.

- ❑ Both types of template create a folder under the Workspaces node.
- ❑ Enterprise group administrators can see all users in the system and add anyone to the groups they manage. Tenant group administrators can only see users who belong to their groups.
- ❑ The Enterprise Resource template creates a Shared Enterprise Portal with the name enterprise and a URL .../ibi\_apps/bip/portal/enterprise.
- ❑ By contrast, the Tenant Resource template creates a Shared Tenant Portal with the name multitenant and a URL .../ibi\_apps/bip/portal/multitenant.

Both kinds of template create the following groups:

- ❑ Basic Users
- ❑ Advanced Users
- ❑ Developers
- ❑ Group Administrators

The rules applied to these groups form a default security policy. Functional capabilities within the workspace increase respectively for basic users, advanced users, and developers. Group administrators do not have the ability to run reports, but they can manage the ownership of resources and manage group membership within their workspace. In organizations where an individual has more than one role, the user account can be added to all the groups necessary to achieve the desired blended set of privileges.

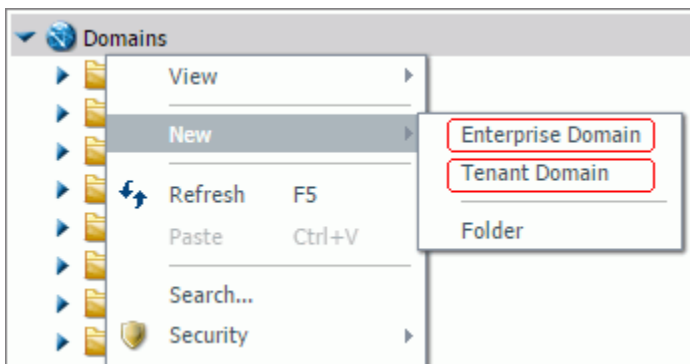
These templates also create rules on the Workspaces, Portals, and Reporting Servers nodes. For more information about the default rules, see [Creating a Custom Resource Template](#) on page 391.

## Enabling or Disabling Built-in Resource Templates

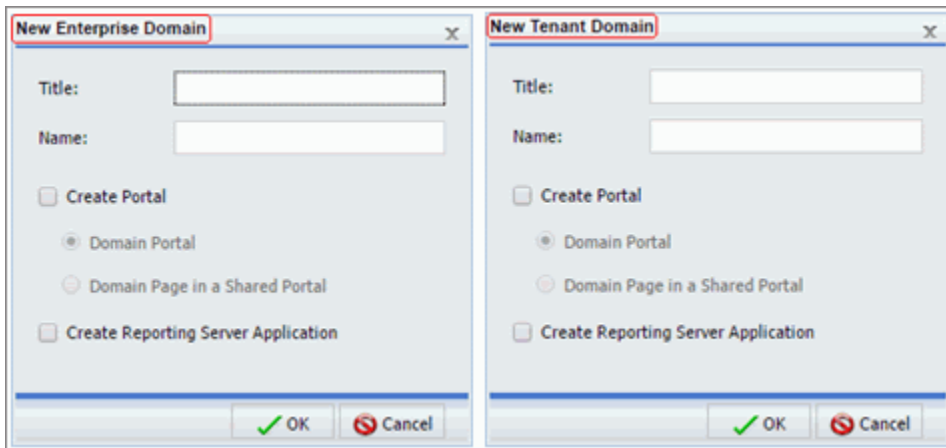
WebFOCUS ships with a set of six resource templates for enterprise workspaces and a set of six resource templates for tenant workspaces. Both sets are enabled, by default. The type of workspace and options available for selection when creating a workspace, determines the resource template that runs and the resources that are created for it.

Even though you can create a new workspace from the WebFOCUS Home Page, in order to take advantage of the full range of resources when doing so, we recommend that do so from the Legacy Home Page.

To create a new enterprise workspace or a new tenant workspace, sign in as an administrator, and open the Legacy Home page. In the BI Portal Resources tree, right-click the *Workspaces* node, and point to *New*, as shown in the following image.



Depending on the type of Workspace you select, one of the following similar looking dialog boxes appears.



This initial selection of Enterprise Workspace or Tenant Workspace, and the additional options you select from the dialog boxes, invokes one of the following underlying resource templates:

### Enterprise Workspaces

- ☐ Enterprise Workspace

- ☐ Enterprise Workspace (Shared Portal)
- ☐ Enterprise Workspace (with Portal)
- ☐ Enterprise Workspace and Application
- ☐ Enterprise Workspace and Application (Shared Portal)
- ☐ Enterprise Workspace and Application (with Portal)

### **Tenant Workspaces**

- ☐ Tenant Workspace
- ☐ Tenant Workspace (Shared Portal)
- ☐ Tenant Workspace (with Portal)
- ☐ Tenant Workspace and Application
- ☐ Tenant Workspace and Application (Shared Portal)
- ☐ Tenant Workspace and Application (with Portal)

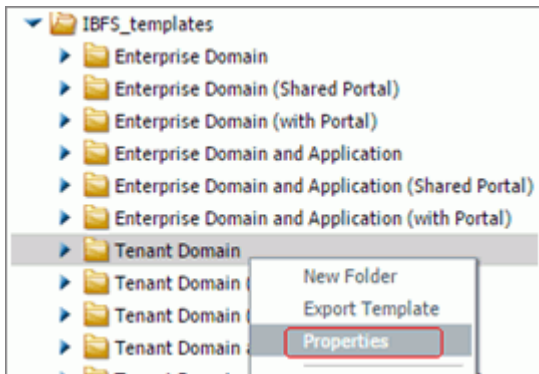
Typically, a WebFOCUS environment is either configured to support an enterprise deployment model or a SaaS tenant deployment model, but not both. As such, an administrator might want to disable an entire set of resource templates to prevent the display of the non-supported model on the Workspace node shortcut menu. To disable all SaaS tenant resource templates or all enterprise resource templates, you need to assign the value *false* to the Enabled setting of only one of the templates in the set.

### ***Procedure:* How to Disable a Group of Built-In Resource Templates**

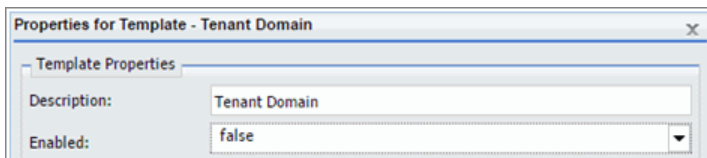
This feature is only available from the Legacy Home Page.

1. Sign in as an administrator, and open the Legacy Home Page.
2. In the Resources tree, right-click the *Workspaces* node, point to *View*, and then click *Full View*.
3. In the Resources tree, expand the *File* folder, and then expand the *IBFS\_templates* folder.

4. Right-click a folder and click *Properties*. For example, click the *Tenant Workspace* folder, as shown in the following image.

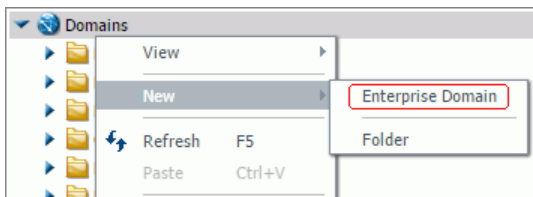


5. In the Properties for Template dialog box Enabled list, click *false*, as shown in the following image.



6. Click *OK*.
7. Right-click the *Workspaces* node, point to *View*, and then click *Repository View* to restore the Resources tree to its original view.
8. Right-click the *Workspaces* node, and point to *New*.

Only the Enterprise Workspace command appears in the shortcut menu, as shown in the following image.

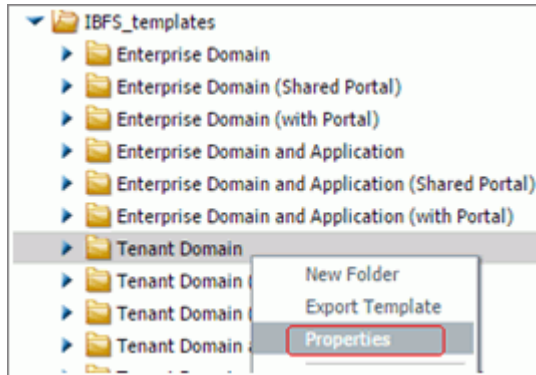


### **Procedure: How to Re-Enable a Group of Built-In Resource Templates**

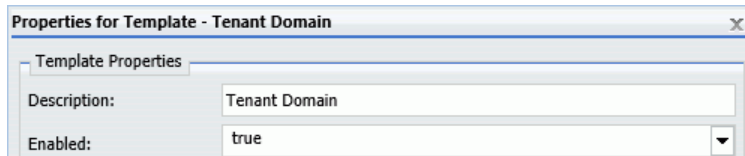
If a hidden group of Resource Templates must be restored, an administrator must reset the Enabled list value to *true* for the previously-disabled resource template.

This feature is only available from the Legacy Home Page.

1. Sign in as an administrator, and open the Legacy Home Page.
2. In the Resources tree, right-click the *Workspaces* node, point to *View*, and then click *Full View*.
3. Expand the *File* folder, and then expand the *IBFS\_templates* folder.
4. Right-click the folder whose Enabled property was previously set to *false* to hide the entire group of templates, and then click *Properties*. For example, right-click the *Tenant Workspace* folder as shown in the following image.



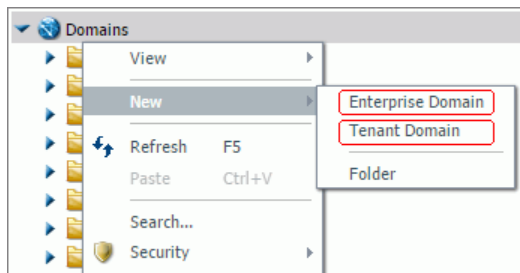
5. In the Properties for Template dialog box Enabled list, click *true*, as shown in the following image.



6. Click *OK*.
7. Right-click the *WebFOCUS* node, point to *View*, and then click *Repository View* to restore the Resources tree to its original view.
8. Right-click the *Workspaces* node, and point to *New*.



Both the Tenant Workspace and the Enterprise Workspace commands appear in the shortcut menu, as shown in the following image.



## Deleting Workspaces

A workspace can only be deleted by an administrator who has rights to delete all of the resources within it.

When you delete a workspace, the resources associated with it are also deleted. This means the workspace group and its subgroups are deleted. Other optional resources that may have been created with the workspace are also deleted, for example, if the workspace references:

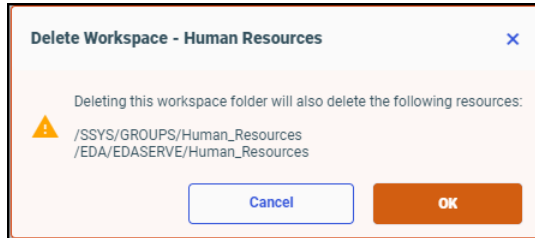
- ☐ A portal, that portal will be deleted.
- ☐ Pages in a shared portal, the pages created with that workspace will be deleted.
- ☐ A WebFOCUS Reporting Server application, that application will be deleted.

**Notes:** The cascade delete process only removes users from groups within a workspace. It does not delete the users themselves.

### **Procedure:** How to Delete a Workspace

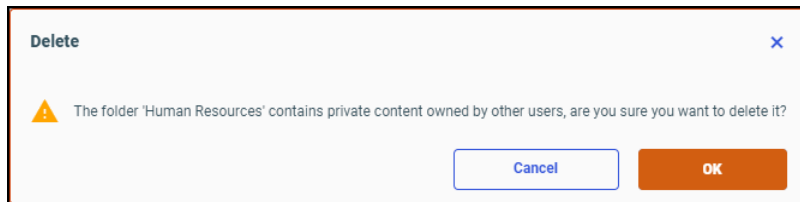
1. Sign in as an administrator.
2. Open the Workspaces view from the Hub or the WebFOCUS Home Page and expand the Resources tree.
3. In the Resources tree, under Workspaces, or in the content area, under Folders, right-click a workspace folder, and then click *Delete*.

4. When you receive a message advising you that this process will delete all resources created by this workspace folder, click **OK** to delete the workspace and associated resources, as shown in the following image.



**Note:** In this message, the list of resources that will be deleted depends upon the resources that were originally included in the workspace. Therefore, the details in this message will vary with each deleted workspace.

5. If you receive a message warning that the folder contains private content, as shown in the following image, click **OK** to delete the workspace and its private content, or click *Cancel* to end the process without deleting the workspace.



### Managing Workspace Users After Deleting a Workspace

Even though deleting a workspace automatically deletes the groups associated with it, this action does not delete the users assigned to those groups. Users from the deleted groups remain in the Users pane in the Security Center. If users from deleted groups are no longer needed, an administrator can delete them from the Repository. For more information see, [How to Delete a User](#) on page 452.

### Customizing Resource Templates

The predefined roles created by resource templates can be customized in the Security Center. For example, if you want your Advanced Users to be able to use InfoAssist only from Reporting Objects, but not with metadata, you can remove the *InfoAssist from Metadata* privilege from the Advanced User role.

Running the resource template does not overwrite roles that already exist. Any customizations that you made to the workspace roles are retained and apply to users in all workspaces, including those previously created.

**Note:** Roles are checked when users sign in. Therefore, changes to user roles take effect immediately for users who sign in after you save the role changes. Users who are signed in when you change a role may need to sign out and sign back in again for the changes to take effect.

For more information about how to modify roles, see [Managing Roles](#) on page 463.

## Creating a Custom Resource Template

Custom resource templates are adaptations of standard resource templates designed to support a unique set of business or operating requirements. Workspaces created from custom resource templates conform to a specialized combination of rules and resources. Custom resource templates help ensure that the privileges and resources required by a particular group or activity are automatically built in to all of the workspaces created for their support.

To create a custom resource template, an administrator generates a workspace that combines the resources and deployment type, Enterprise or Tenant, that best suits the proposed custom resource template, creates a folder for it, and makes a copy of the standard template scenario.xml file whose combination of resources and deployment best match those of the workspace.

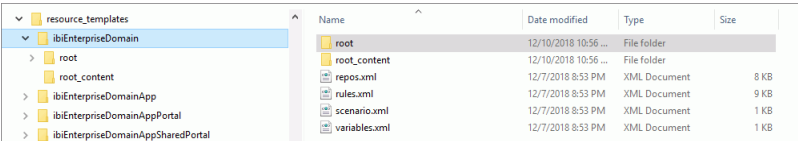
When these three components are ready, the administrator exports the scenario.xml file in the custom template folder to create the full set of files for a resource template. The Title and Name assigned to the workspace become the Title and Name of the new template and are added to the Workspaces node shortcut menu to enable users to select the custom resource template when they create new workspaces.

In addition to these basic steps, administrators can customize the privileges or roles assigned to a custom resource template, and arrange variables and the order in which they are displayed.

Before you create a custom template, it is important to understand the concepts such as privileges, roles, resources, groups, and IBFS subsystems. For more information about these features, see the corresponding topics in [User Administration](#) on page 443. You should also review the resource templates already included in your installation in order to become familiar with possible combinations of privileges, roles, and rules.

Resource Template Location and Files

By default, both built-in and custom resource templates are contained in the resource\_templates folder, located in drive:\ibi\WebFOCUS82\config\ for Windows or install\_directory/ibi/WebFOCUS82/config/ for UNIX or Linux, as shown in the following image.



If you are using the integrated installation, drive:\ibi\WebFOCUS\_WFI\WebFOCUS\config \resource\_templates\ibiEnterpriseDomain for Windows or install\_directory/ibi/WebFOCUS\_WFI/ WebFOCUS/config/resource\_templates/ibiEnterpriseDomain for UNIX or Linux.

In the IBFS system, resource templates are located on the Legacy home page in the Resources tree under WebFOCUS /FILE/IBFS\_templates. This path is visible when the Resources tree is converted to Full View mode.

The following table describes the resources created in each resource template folder.

Name	Type	Purpose
root	Directory structure	Contains resources, such as report procedures or portal pages. Some subdirectories may be empty, but they are required.
repos.xml	File	Specifies the properties of all resources created by the template.
reposTree.xml	File	Lists the resources that have been exported into the template for troubleshooting or documentation purposes. This file is automatically created when a template is created, but it is not required when a template is run. <b>Note:</b> This file is not included in the resource templates.
rules.xml	File	Specifies the security rules created by the template.

Name	Type	Purpose
scenario.xml	File	Specifies the information necessary to create a resource template. This file is often distributed with a resource template to aid in the creation of a custom template, but is not required when a template is run.
variables.xml	File	Specifies how the resource template prompts for required information. Items specified include the name of each prompt, the prompt sort order, and the type of prompt field (normal or check box).

## Resource Template Variables

When you use a resource template, WebFOCUS determines whether the template contains any variables, and prompts you to provide a value for each variable, if necessary. You can specify the names, descriptions, and titles of resources, such as folders, groups, portals, and portal pages. You can also provide the summaries of folders or items that will appear to users or administrators.

For example, your template can include an IBFS content folder with a predetermined name and description. The folder can be empty, or it can contain subfolders and some content. The folder itself can also have folder properties defined, such as the Sort Order and Auto Create My Content Folders properties. When this resource template is run, you will be prompted for the title and name to use in the creation of this folder.

The Resource Template Management interface allows you to supply a user-friendly display description for variables. You can also specify the order in which the variables are shown in the template dialog box and the type of variable to display.

The following table describes the types of variables that are used with resource templates.

Variable Type	Purpose
normal	This type of variable is typically used for the description of groups or for the title of folders and portal pages seen by the end user. Any alphanumeric data is allowed in a normal variable.

Variable Type	Purpose
check	This type of variable is typically used for the name of IBFS resources. Data supplied to a check variable is validated against the rules for components of an IBFS path.

Creating a Model Using the Enterprise Resource Template

You can export any IBFS resources and security rules you wish into a custom resource template. First, you must create the resources and rules that you wish to use in your custom template. For example, you might wish to create a department-specific group with subgroups for each business role, along with a department-specific content folder. You might also wish to give all users access to a common content folder and portal, or to include custom roles in the template.

When you have finished making changes, you can export the custom template for later use.

Procedure: How to Create a Resource and Policy Model

This feature is only available from the Legacy Home Page.

1. Open the Legacy Home Page.
2. On the BI Portal, in the Resources tree, right-click the *Workspaces* node, point to *View*, and then click *Repository View*.
3. Right-click the *Workspaces* node, and point to *New*.
  - ☐ Click *Enterprise Workspace* to create a custom template for department or division workspaces within an enterprise.
  - ☐ Click *Tenant Workspace* to create a custom template for workspaces for clients of a SaaS provider.
4. Type `%%desc%%` in the Title field.

As you type, the `%%desc%%` value is automatically assigned to the Name field.
5. Type `%%name%%` in the Name field using lowercase characters.
6. To include optional resources in the model workspace, perform the following steps:
  - a. To include a portal, select the *Create Portal* check box, and then click *Workspace Portal*.
  - b. To include shared portal pages, select the *Create Portal* check box, and then click *Workspace Page in a Shared Portal*.

- c. To include an associated application directory on the WebFOCUS Reporting Server, select the *Create Reporting Server Application* check box.

**Note:** When using the Create Reporting Server Application option, we recommend that you develop a strategy for authorizing workspace users to the Application Directories on the WebFOCUS Reporting Server. For more information, see [Understanding Access Control Templates](#) on page 401.

7. Click *OK*.
8. When you receive a confirmation message stating that resource template processing is complete, click *OK*.

The Workspaces Node now includes a content folder titled %%desc%%. The content folder contains a My Content and a Hidden\_Content folder. If you included additional resources, such as a portal, these resources appear on the Resources tree as well.

9. To review the rules in place, right-click the new content or portal resource, point to *Security*, and then click *Rules on this Resource*.

By default, the rules on this resource dialog box will display rules for the four basic workspace user groups and Managers.

### **Procedure:** How to Create the Custom Template Folder

By default, only administrators are authorized to run and create resource templates.

This feature is only available from the Legacy Home Page.

1. Open the Legacy Home Page.
2. On the BI Portal, right-click the *Workspaces* node, point to *View*, and then click *Full View*.
3. Expand the *FILE* folder, right-click the *IBFS\_templates* folder, and then click *New Folder*.
4. Type the name of your new template in the Title field and a brief description of the template in the Summary field.

The name will be the IBFS name of your custom template. You will be able to modify the display title of the template later.

**Note:** The template name must follow the conventions for IBFS names. For example, spaces are replaced with underscores (\_). For more information about IBFS naming conventions, see [IBFS Filesystem and Subsystems](#) on page 340.

5. Click *OK*.

A folder with the name of your new template appears under the *IBFS\_templates* node.

## Procedure: How to Copy a scenario.xml File for the Custom Template

The scenario.xml file tells WebFOCUS what to export into your custom resource template. Before you can make any customizations, you must move a copy of the scenario.xml file that best fits the resources needed for the custom resources template from the model template folder to the Custom Resource folder. Once you have created a copy of the standard resource template xml file, if you choose to use a different Name or Title for workspaces created from this template, you need to update the values assigned to the scenario.xml file as described in the topic, [How to Update the Scenario File](#) on page 398.

This feature is only available from the Legacy Home Page.

1. Under the IBFS\_Templates folder, expand the folder containing the template that most closely matches the type of workspace and resources you want to create.

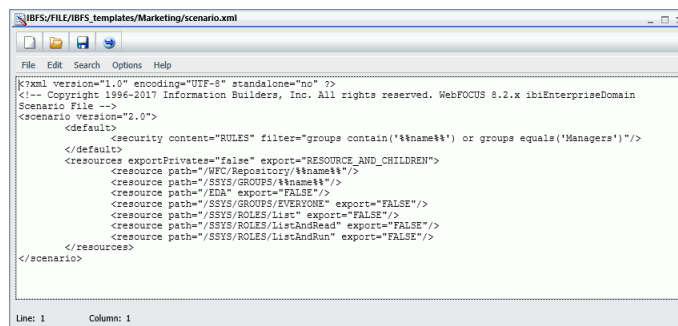
The folder you select must match the configuration of workspace type and resources you selected when creating the model workspace. For example, if the model workspace is an Enterprise Workspace with no additional resources, copy the scenario.xml file from the Enterprise Workspace folder.

2. Right-click the *scenario.xml* file in your selected folder, and then click *Copy*.
3. Right-click the new custom template folder, and then click *Paste*.

The custom template folder displays a copy of the scenario.xml file.

4. In the new custom template folder, right-click the *scenario.xml* file, and then click *Edit*.

The text editor opens and displays the contents of the scenario.xml file for your selected template type. In this example, the scenario.xml file for the enterprise resource template, as shown in the following image.



Attributes in the security tag apply additional filters to the rules that will be exported when creating workspaces based on this custom template. In this example, the custom template will only export the Rules on EDA, in which the subject matches %name% or Managers.



The resources section specifies that private content will not be exported and that specified resources and their descendants will be exported. Each resource related to the template is specified by its full IBFS path. In some cases, the resource path name is parameterized, such as /WFC/Repository/%%name%%. In other cases, a static path name is specified, such as /SSYS/ROLES/List. When you wish to export the rules on a subsystem, but not the resources it contains, specify the resource path with the export="FALSE" option.

**Note:** Any new variables included must be in lowercase.

5. When your review is complete, close the text editor.

## Adding Customizations to the Custom Resource Template

You can update the roles and rules assigned to the custom template.

This feature is only available from the Legacy Home Page.

### **Procedure:** How to Disable Auto Create My Content Folders

The model folder created by the Enterprise Resource template allows users to save personal content into top-level folders. You may wish to disable this feature in your custom template.

Even though this setting is visible on the Advanced tab of the Properties panel that opens from the Workspaces area that opens from the Hub or the WebFOCUS Home Page, we recommend that you make this change in the Legacy Home Page environment.

This is one of only several customizations you can make to the custom resource template.

1. Right-click the Workspace folder created from a custom template, and then click *Properties*.
2. In the Properties dialog box, clear the *Auto Create My Content Folders* check box, and save your changes.

### **Procedure:** How to Enable Access to a Common Portal or Folder

You may wish to grant groups created by your template access to an existing portal or content folder. If everyone will have the same access privileges, you can create a rule granting SSYS/GROUPS/EVERYONE an appropriate role for the use of the common resource. If you prefer not to include this rule in the template, but wish to use it later, you can create this rule or any other rule later.

This feature is only available from the Legacy Home Page.

To enable access to a common portal or folder:

1. Create the common portal or folder.

You do not need to design the portal or populate the folder at this point. You just need it to exist so you can set rules on it.

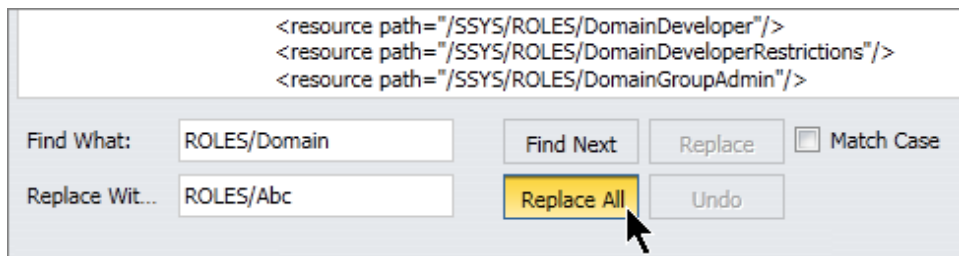
2. Right-click the resource, point to *Security*, and then click *Rules*.
3. Select a group, and click a role and access type.
4. Click *Apply*, and then click *OK* to close the window.

### **Procedure:** How to Update the Scenario File

This feature is only available from the Legacy Home Page.

1. With the Resources tree in Full View mode, expand the *FILE* node, then expand the *IBFS\_templates* node, then expand your template folder.
2. Right-click the *scenario.xml* file and click *Edit*.

If you created custom roles, you can use search and replace to globally rename the role resources in the file. For example, you can replace SSYS/ROLES/Workspace with SSYS/ROLES/Abc, as shown in the following image.



3. Make your changes and click *Save*.
- Note:** IBFS path names are case-sensitive.
4. When your changes are complete, click *Save*.
  5. Click *File*, and then click *Exit* to close the file.

## Exporting the Custom Resource Template

When all customizations are complete, export the template.

### **Procedure:** How to Export a Custom Resource Template

This feature is only available from the Legacy Home Page.

1. Open the Legacy Home Page.
2. With the Resources tree in Full View, right-click your template folder, and then click *Export Template*.

3. When you receive a confirmation that template processing is complete, click *OK*.
4. Right-click the template folder and click *Refresh* to see the new resources.

## Updating Resource Template Properties

To update the properties of a resource template, right-click the template folder, and then click *Properties*. The Properties for Template dialog box appears, as shown in the following image.

The screenshot shows a dialog box titled "Properties for Template - AbcDomain". It contains two main sections: "Template Properties" and "Variable Properties".

- Template Properties:**
  - Description: Abc Corp Domain
  - Enabled: true (dropdown menu)
  - Sort Order: (empty text field)
- Variable Properties:**
  - Variable: desc**
    - Description: Description
    - Sort Order: 2
    - Type: normal (dropdown menu)
  - Variable: name**
    - Description: Name
    - Sort Order: 1
    - Type: check (dropdown menu)

At the bottom right, there are "OK" and "Cancel" buttons.

The Properties for Template dialog box allows you to edit the template description and sort order, and to enable or disable the template to show it or hide it in the list of available templates. You can also change the descriptions of the variables shown in the specific template dialog box, determine their sort order within the template dialog box, and configure what type of variable they are.

**Note:** If a variable prompts for values used in the IBFS path name or a resource, set the Variable Type to *Check* to ensure that unsupported IBFS characters for the value are rejected.

### Removing the Model

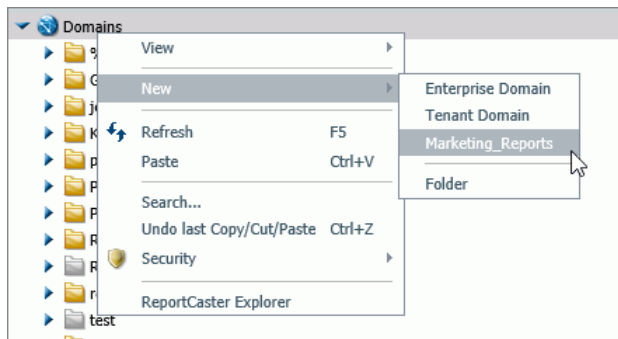
Once you have exported your resource template, the resource and policy model objects in your repository are no longer needed. You can leave them in place if you plan to re-create your template in the future or if you wish to create additional variants of the template. Otherwise, you can delete the model objects at this point. You can always re-create them again in the future with your template.

### **Procedure:** How to Test the New Custom Resource Template

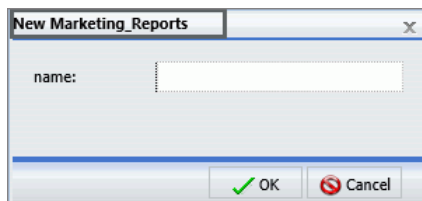
To test the presence of the new custom resource template in the Workspaces node, you must ensure that a command for it appears on the Workspace node shortcut menu, and that the Create Workspace dialog box includes the name of the custom template in the title.

This feature is only available from the Legacy Home Page.

1. In the BI Portal, right-click the *Workspaces* node, and point to *New*.
2. Ensure that the name of the Custom Resource template appears on the New submenu, as shown in the following image.



3. Click the name assigned to the Custom Resource Template such as, *Marketing\_Reports*.
4. Ensure that the title above the Create a Workspace dialog box contains the name of the custom resource template, as shown in the following image.



5. Create the workspace as described in [How to Create a Workspace](#) on page 379.

Review the new workspace to ensure that the resources and privileges it contains conform to those of the custom resource template.

## Understanding Access Control Templates

WebFOCUS Reporting Server Access Control Templates, in conjunction with WebFOCUS Resource Templates, provide a comprehensive access control solution for users in an Enterprise or SaaS Tenant deployment.

Access Control Templates are configurations of groups, roles, and privileges that, when defined on a WebFOCUS Reporting Server, automatically grant users in those groups an appropriate level of access to the application directories and capabilities available on that server. For example, a user assigned only to the Marketing/AdvancedUsers group can create reports using metadata residing in the marketing application directory, but not metadata residing in the finance application directory. Another user, assigned to the Marketing/Developers group, can access Reporting Server browser interface tools to monitor their connections and agents, while other marketing users who are not in that group, cannot.

If you only need to support a small number of groups, you can use the Reporting Server browser interface to create individual application directories manually, and then configure access privileges for each one. However, when there is a pattern of access between group names and application directories, the implementation of server access control templates is a best practice that saves time, imposes consistency on the results, and is easy to use. Server access control templates allow for the best integration of resource templates with application directory access privileges and the assignment of users to their proper server role.

However, note that explicit group registration takes precedence over access control template matching. A user connecting to the WebFOCUS Reporting Server from a group that maintains an explicit registration on the WebFOCUS Reporting Server, will always obtain their authorization from that group, and not from the group that is the closest match in the access control template.

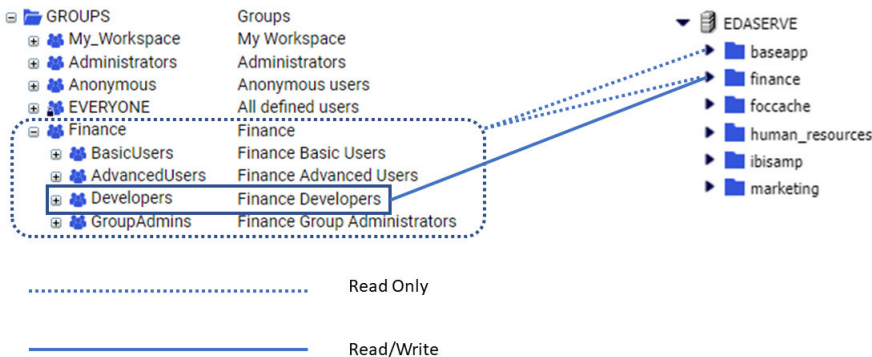
The access control template described in this section follows a standard model for user access. In that model, workspaces created from resource templates create four sub-groups, by default, basic users, advanced users, developers, and group administrators. These four sub-groups enable administrators to tailor the availability of workspace resources to the needs and responsibilities of the four most common user types.

Developing Business Requirements for Server Access Control Templates

The first step in developing an access control template is to develop business requirements that identify the groups, the content with which they are allowed to work, and the appropriate level of access to that content. For the access control template discussed in this section, consider the following business requirements:

- 1. All users have read-only access to the ibisamp directory and the baseapp directory.
- 2. Managers and Administrators have read/write access to the application directories of all workspaces.
- 3. Workspace users have read-only access to the application directory for their workspace.
- 4. Workspace developers have read/write access to the application directory for their workspace.
- 5. Workspace users and developers have no access to any directories other than the application directory for their workspace and the ibisamp and baseapp directories.

These business requirements are shown in the following image. In this example, workspace users and developers are assigned to the Finance workspace. For clarity, the Administrator and Manager access lines are omitted.



When you configure an access control template, you can vary these basic requirements. For example, if all users do not need to have access to the ibisamp directory or the baseapp directory, you can remove the option that grants access to those directories to all users.

The business requirements listed in this example are the basis for the access control template configuration that appears in the Access Control Template Text section and throughout the remainder of this section.

## Access Control Template Regular Expressions and Group ID Patterns

Regular expressions and Group ID patterns make access control templates available to a range of groups. As long as the name of a group matches a Group ID pattern, the template and its configuration of WebFOCUS Reporting Server access roles and privileges automatically applies to that group. The regular expressions used to configure Group ID patterns allow administrators to limit an access control template to a select few groups that conform to a closely-defined pattern, or to make a template accessible to a broad range of groups that conform to a minimally-defined pattern. By default, these regular expressions include:

- ❑ The **(.+)** pattern captures all group names. This pattern contains the following elements:
  - ❑ The wildcard **(.)** matches any character, including those in extended character sets.
  - ❑ The plus sign quantifier **(+)** indicates that the preceding wildcard matches one or more characters.
- ❑ The **(.+)/Developers** pattern captures the Developers groups within all workspaces. In this pattern, the **/Developers** term limits the **(.+)** pattern to those groups whose name ends with the **/Developers** character string. For example, **Retail\_Samples/Developers**.

Access control templates also use two placeholder terms as variables in their configuration.

- ❑ **modelgrp**. Causes the expressions in which it appears to capture all groups. These groups assume the Basic User role. Groups whose names conform to the pattern, *modelgrp/developers*, assume the Application Administration Role.
- ❑ **modelapp**. Causes the expressions in which it appears to capture all applications.

In this configuration example, these values are assigned to fields on the Template Registration page of the WebFOCUS Reporting Server browser interface. They also appear in the configuration file that records access control template settings.

## Creating Access Control Templates

The access control template feature is compatible with many different authentication and authorization configurations. However, the topics in this section presume the use of Internal Authentication, and pass groups through a trusted connection to the WebFOCUS Reporting Server for user authorization.

There are two different ways to configure an access control template:

- ❑ **Copy and Paste.** Copy the access control template text from this document, and paste it into the admin.cfg file on the WebFOCUS Reporting Server.

This method creates access templates quickly, and it is most efficient when few or no changes to this sample template are required to adapt the configuration of group permissions it contains to your installation.

- ❑ **Manual Configuration.** Configure the environment in the Reporting Server browser interface, and generate an access control template from it.

This method requires more time and effort, and it is most efficient when the requirements for a new access control template cannot be based on this standard template.

### Access Control Template Prerequisites

Before creating access control templates, regardless of the method you choose, you must:

- ❑ Allow the WebFOCUS client to pass Trusted User IDs and Groups to the WebFOCUS Reporting Server by configuring the WebFOCUS Reporting Server Security setting in the WebFOCUS Client Administration Console.
- ❑ Allow the WebFOCUS Reporting Server to accept those Trusted User ID and Groups by changing the Security Provider Trusted setting to *y* (Yes) on the Reporting Server browser interface.
- ❑ Restrict Trusted Connections to specific hosts by changing the Special Service and Listener configuration on the Reporting Server browser interface to accept hosts that support trusted communications.
- ❑ Disable the automatic pre-pending of the name of the primary security provider when registering group or user names by changing the value in the Console Access Control setting, `prepend_provider_name` setting, located on the Access Control page of the Reporting Server browser interface, to *n* (No). By disabling this setting, you can switch to another primary security provider later if, for example, you want to authenticate users to the Active Directory instead of Internal Authentication, without re-registering those users or group roles.

You will find instructions on how to configure these prerequisites in the following topics.

The features that support this configuration are most readily available from the Legacy Home Page.



**Procedure: How to Establish a Trusted Connection to the WebFOCUS Reporting Server From the WebFOCUS Client**

This procedure is based on the default configuration of internal authentication and authorization. The features that support this procedure are only available from the Legacy Home Page.

To confirm that your installation uses internal authentication and authorization, on the Administration Console Security Tab, under the Security Configuration folder, click *External*. If the Enable External Security check box is cleared, your installation uses internal authentication. If the Internal option in the User Authorization group is selected, your installation uses internal authorization. If you identify a different configuration, contact the Customer Support Team for information on establishing a trusted connection.

Note that this procedure establishes a trusted connection to the *EDASERVE* WebFOCUS Reporting Server, and not to any other WebFOCUS Reporting Server. This server is specified because the default resource templates also specify *EDASERVE* as the WebFOCUS Reporting Server in their configuration. If you must establish a trusted connection to a different WebFOCUS Reporting Server, you must also replace *EDASERVE* with the name of your chosen WebFOCUS Reporting Server in each of the default resource templates.

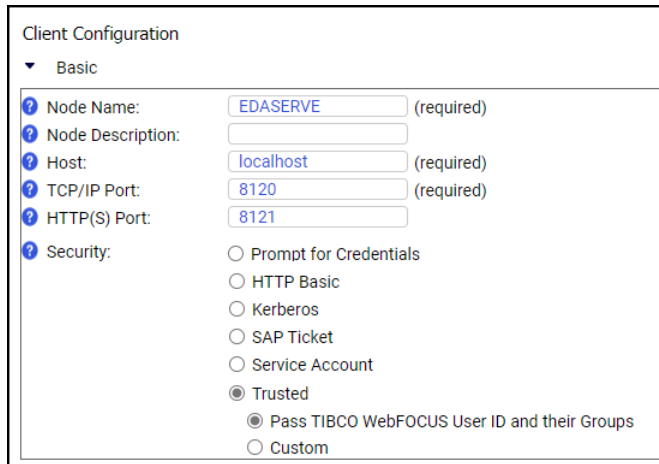
1. In the Administration Console, on the Configuration tab, expand the *Reporting Servers* folder, and then expand the *Server Connections* folder.
2. Double-click the *EDASERVE* node.
3. On the Client Configuration page, under the Security entry, click the *Trusted* option.

The page refreshes and displays two options. The Pass WebFOCUS User ID and their Groups option is selected automatically.

4. In the Host field:
  - a. If the WebFOCUS Client and WebFOCUS Reporting Server are on the same machine, type *localhost*.
  - b. If the WebFOCUS Client and WebFOCUS Reporting Server are on different machines, type the name or IP address of the machine hosting the WebFOCUS Reporting Server.

You will later assign this same value to the *RESTRICT\_TO\_IP* setting on the WebFOCUS Reporting Server to disallow trusted connections from other clients.

5. Review your configuration to ensure that it resembles the following image:



The screenshot shows the 'Client Configuration' dialog box with the 'Basic' tab selected. The configuration fields are as follows:

Field	Value	Requirement
Node Name:	EDASERVE	(required)
Node Description:		
Host:	localhost	(required)
TCP/IP Port:	8120	(required)
HTTP(S) Port:	8121	(required)
Security:	<input type="radio"/> Prompt for Credentials <input type="radio"/> HTTP Basic <input type="radio"/> Kerberos <input type="radio"/> SAP Ticket <input type="radio"/> Service Account <input checked="" type="radio"/> Trusted <div><input checked="" type="radio"/> Pass TIBCO WebFOCUS User ID and their Groups <input type="radio"/> Custom</div>	

**Note:** Ensure that localhost has been replaced by the Host Name of the WebFOCUS Reporting Server, if the WebFOCUS Client and WebFOCUS Reporting Server are on different machines.

6. Click Save.
7. When you receive a message that the WebFOCUS Reporting Server update was saved successfully, click OK.
8. On the Administration Console Menu bar, click *Clear Cache*.
9. When you receive a message that all caches are cleared, click OK.
10. Sign out of your current session.

### **Procedure:** How to Identify the Security Provider as a Trusted Security Provider

In order for the Access Control features to function, you must run the WebFOCUS Reporting Server with a Security Provider. This provider could be PTH<Internal>, LDAP, OPSYS, DBMS, or a CUSTOM provider, such as one that authorizes users to access a relational database management system (RDBMS).

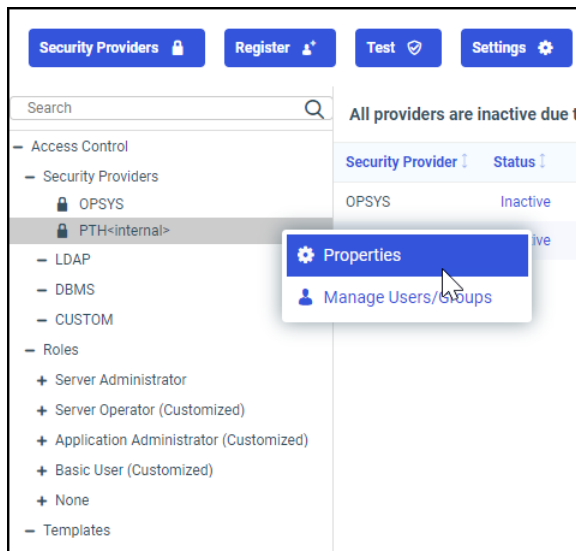
1. From the Hub side navigation pane, select *Management Center*, and *Access Control*.

Or

From the WebFOCUS Home Page, select *Settings* and *WebFOCUS Server* to open the Reporting Server Browser interface. On the Menu bar, select *Tools* and *Access Control* to open the Access Control page.

- Under the Access Control folder, right-click the node of the current security provider for the WebFOCUS Reporting Server, and then click *Properties*.

For example, right-click *PTH <internal>* , and then click *Properties*, as shown in the following image.



**Note:** The OPSYS provider does not allow trusted communications on Windows platforms.

- On the configuration page of your selected security provider, scroll down to the `trust_ext` list and confirm that the value `y` appears. If not, click `y` in the `trust_ext` list, and then click *Save*.

For example, on the Security Configuration PTH<internal> page, click *y* in the *trust\_ext* list, and then click *Save*. When the properties panel closes, click *Save and Restart Server*, as shown in the following image.

The screenshot shows the 'Security Configuration PTH<internal>' page. It features a list of configuration options on the left, each with a dropdown menu or input field. The options are: *authenticate\_all\_ptuser?* (dropdown with 'y'), *pthpass\_casesensitive?* (dropdown with 'n'), *pthpass\_mixedchars?* (dropdown with 'n'), *pthpass\_lifetime?* (input field with '60' and 'days' label), *pthpass\_length?* (input field with '0' and 'characters' label), *pthpass\_unique?* (input field with '0' and '# passwords' label), *pthpass\_lockout?* (input field with '0' and 'failures' label), *pthpass\_lockout\_duration?* (input field with '0' and 'minutes' label), and *trust\_ext?* (dropdown with 'y'). The *trust\_ext?* dropdown is highlighted with a red rectangle. At the bottom right, there is a blue button labeled 'Save and Restart Server' with a mouse cursor pointing at it.

The WebFOCUS Reporting Server stops and restarts automatically.

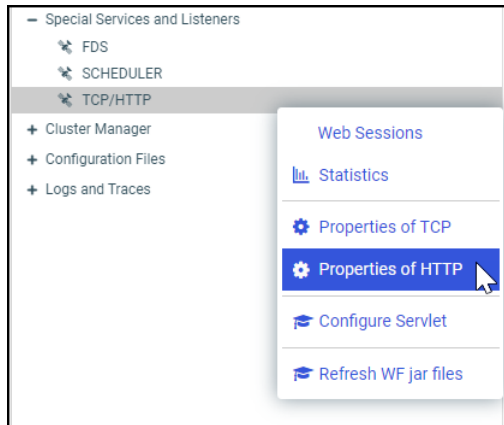
**Note:** The PTH<Internal> security provider is configured as a trusted security provider, by default. If you select a different security provider that has not been configured, you must complete the configuration first. For more information see the Configuring Authentication section of the *TIBCO WebFOCUS® Reporting Server Administration Manual*.

4. When you receive the Workplace Restarting message, stand by.
5. Select *Tools* and *Access Control*, right-click *PTH<Internal>*, and review the new trusted configuration.

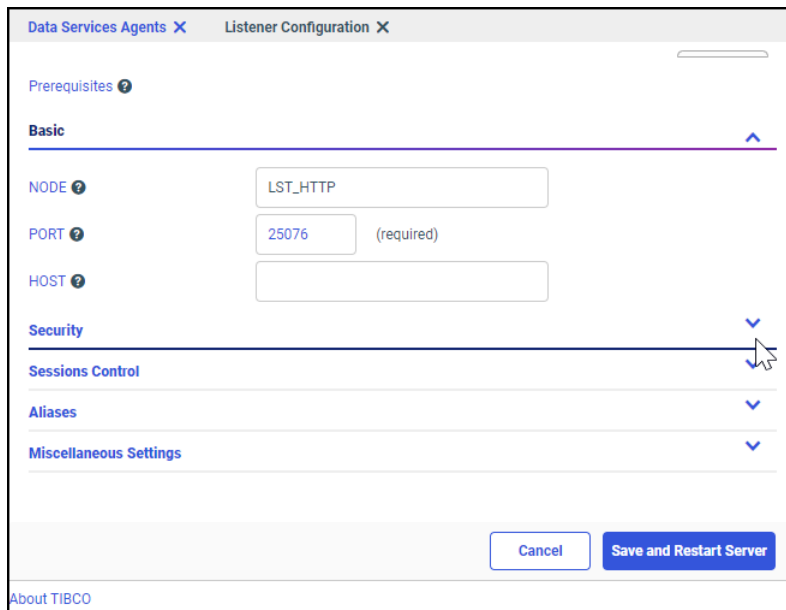
### **Procedure:** How to Restrict Trusted Access to Specific Hosts

1. Open the Reporting Server browser interface, and open the Workspace page.
2. In the Workspaces tree, expand *Special Services and Listeners*.

3. Right-click the *TCP/HTTP* node, and then click *Properties of TCP*, as shown in the following image.



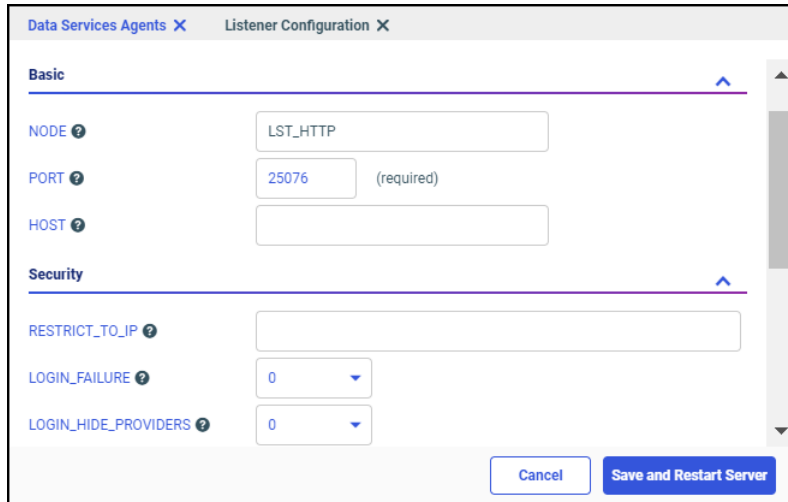
4. Expand the *Security* header, as shown in the following image.



5. If the WebFOCUS Reporting Server is on the same host machine as the WebFOCUS Client and Distribution server, type *localhost* in the *RESTRICT\_TO\_IP* field.

If the WebFOCUS Reporting Server is *not* on the same host machine as the WebFOCUS Client and Distribution server, type the TCP/IP addresses or names of all of the WebFOCUS Clients and the Distribution Servers that will be used to access this WebFOCUS Reporting Server.

6. Click *Save and Restart Server*, as shown in the following image.



The screenshot shows a 'Listener Configuration' dialog box with two tabs: 'Data Services Agents' and 'Listener Configuration'. The 'Listener Configuration' tab is active. It has two sections: 'Basic' and 'Security'. In the 'Basic' section, there are three fields: 'NODE' with the value 'LST\_HTTP', 'PORT' with the value '25076' and a '(required)' label, and 'HOST' which is empty. In the 'Security' section, there are three fields: 'RESTRICT\_TO\_IP' which is empty, 'LOGIN\_FAILURE' with a dropdown menu showing '0', and 'LOGIN\_HIDE\_PROVIDERS' with a dropdown menu showing '0'. At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Save and Restart Server'.

7. When the Sign in page opens with the *session lost due to server restart* message, type the server ID and password used in the installation, typically, *svadmin* for both, and then click *Sign In*.

The Reporting Server browser interface reopens and displays the Applications tab.

### **Procedure: How to Disable Primary Security Provider Name Prepending to Group or User Names**

By disabling this setting, you can switch to another primary security provider later if, for example, you want to authenticate users to the Active Directory instead of Internal Authentication, without re-registering those users or group roles.

1. On the Access Control Page, select *Settings* and *Access Control* to open the Access Control Settings tab. Select *n* from the `prepend_provider_name` list, as shown in the following image.

The screenshot shows the 'Access Control Settings' window. Under the 'General' tab, the 'prepend\_provider\_name' dropdown is set to 'n'. The 'Web Console Anonymous Access' section contains three input fields: 'anonymous\_id', 'anonymous\_pass', and 'confirm password'. An 'Apply and Restart Server' button is located at the bottom right.

This setting specifies that when registering groups or users for the primary provider, the provider name is not prepended to the group or user name. This configuration change will allow an administrator to enable a different security Provider, such as Active Directory or LDAP, at a later date, without breaking the connection of the already registered users and groups.

2. Click *Apply and Restart Server*.

After you receive the Workspace restarting please wait message, the WebFOCUS Reporting Server restarts, and the Reporting Server browser interface returns you to the Applications tab.

If the Sign in page opens with the Session lost due to server restart message, type the server ID and password used in the installation, typically, `srvadmin` for both, and then click *Sign In*.

3. Close the Reporting Server browser interface, and sign out.

## Choosing an Access Control Template Creation Method

When the prerequisites are configured, you can use one of two methods to create an access control template.

To create a template by copying and pasting text that is provided in this section, continue with the topic, [Creating Access Control Templates by Copying and Pasting](#) on page 412.

To create a template by directly configuring and registering all of the groups it will contain, continue with the topic, [Creating Access Control Templates by Manual Configuration](#) on page 417.

## Creating Access Control Templates by Copying and Pasting

As of Release 8.2 Version 01, the WebFOCUS Reporting Server installation automatically creates an administration configuration file, identified as admin.cfg. The following sample of the text in the admin.cfg file, located in *drive:\ibi\profiles*, includes the default configuration, with an operating system userid, and the default PTH<internal> security provider.



**Sample default admin.cfg**

```

admin_id = OPSYS\DOMAIN\operatingsystemuserid
BEGIN
    admin_level = SRV
END
admin_id = PTH\srvadmin
BEGIN
    admin_password = {AES}encryptedpassword
    admin_level = SRV
END
admin_level = APP
BEGIN
    admin_privilege = NODPT,NOSYS,METAP,DATMG,PRSAV,PRDFR,PRRPT,
                    PROUT,MONIT,CHGPW,MONUS,MONGR,KILT3,KILGR,
                    APATH,DBMSC,UPROF,APROF
    admin_privilege = *;ANONE
    admin_privilege = (APPROOT);AREAD,ARWRT,PRRUN,ALIST
END
admin_level = USR
BEGIN
    admin_privilege = NODPT,NOSYS,PROUT,CHGPW,MONUS,KILT3,APATH,
                    DBMSC,UPROF
    admin_privilege = *;ANONE
    admin_privilege = (APPROOT);AREAD,ARWRT,PRRUN,ALIST
END
admin_level = OPR
BEGIN
    admin_privilege = NODPT,NOSYS,MONIT,KILAL,STPSV,CHGPW,MONUS,
                    MONGR,KILT3,KILGR
    admin_privilege = *;ANONE
    admin_privilege = (APPROOT);AREAD,ARWRT,ALIST
END
>>>Replace this line with all lines from the WebFOCUS
Access Control Template Text.<<<
[Access Control]
authenticate_all_pthuser = y
prepend_provider_name = n

```

where:

*operatingsystemuserid*

Is the actual operating system user ID.

*encryptedpassword*

Is the userid password that is encrypted by the WebFOCUS Reporting Server using the key specified in the `cfgfile_cipher`.

By default, the template assigns the **USR** role to all users assigned to the **BasicUsers**, **AdvancedUsers**, and **GroupAdmins** groups of individual workspaces. These groups are usually referred to as *Workspace\BasicUsers*, *Workspace\AdvancedUsers*, and *Workspace\GroupAdmins*, where *Workspace* is the name of the individual workspace to which they are assigned. For example, *Finance\BasicUsers*. When users from those groups connect to the WebFOCUS Reporting Server, they have **Read**, **Execute**, and **List** privileges to resources within their workspace application folder.

The template also assigns the **APP** role to the *Workspace\Developers* group. When users from this group connect to the WebFOCUS Reporting Server, they have **Read**, **Write**, **List**, and **Run** privileges for resources within their workspace application folder, as well as additional privileges that support their role as developers.

To replace this generalized configuration of access control settings with an access control template, copy the text from the following section, *Access Control Template Text*, and paste it into an existing `admin.cfg` file. This addition creates an access control template that grants proper authorization to the **Administrators** group, **Managers** group, and any workspace group that connects to the WebFOCUS Reporting Server through the trusted connection defined in [How to Establish a Trusted Connection to the WebFOCUS Reporting Server From the WebFOCUS Client](#) on page 405.

### **Access Control Template Text**

The access control template that appears in this section applies to all trusted users and groups that connect to the WebFOCUS Reporting Server to which this template is assigned. It uses Group ID patterns and regular expressions to establish a configuration that serves most installations effectively. This template is based on an access model that grants all users **Read**, **List**, and **Run** privileges in the `ibisamp` and `baseapp` directories.

```

admin_group = Administrators
BEGIN
    admin_level = SRV
    admin_description = WebFOCUS Administrators
END
admin_group = Managers
BEGIN
    admin_level = SRV
    admin_description = WebFOCUS Managers
END
admin_group = modelgrp/Developers
BEGIN
    admin_level = APP
    admin_privilege = *;ANONE
    admin_privilege = (APPROOT)/baseapp;AREAD,PRRUN,ALIST
    admin_privilege = (APPROOT)/modelapp;AREAD,ARWRT,PRRUN,ALIST
    admin_privilege = (APPROOT);ANONE
    admin_privilege = ADPTP,NODPT,NOSYS,METAP,DATMG,PRSAV,PRDFR,
        PRRPT,PROUT,MONIT,SRVLG,KILT3,APATH
    admin_privilege = (APPROOT)/ibisamp;AREAD,PRRUN,ALIST
END
admin_group = modelgrp
BEGIN
    admin_level = USR
    admin_privilege = NODPT,NOSYS,PRDFR,PRRPT,PROUT,KILT3,APATH
    admin_privilege = *;ANONE
    admin_privilege = (APPROOT)/baseapp;AREAD,PRRUN,ALIST
    admin_privilege = (APPROOT)/modelapp;AREAD,PRRUN,ALIST
    admin_privilege = (APPROOT);ANONE
    admin_privilege = (APPROOT)/ibisamp;AREAD,PRRUN,ALIST
END
admin_group_template = (.+)/Developers
BEGIN
    model_group = modelgrp/Developers
    file_replace_pattern = (modelapp)
END
admin_group_template = (.+)
BEGIN
    model_group = modelgrp
    file_replace_pattern = (modelapp)
    exclude_groups = (/)
END

```

### **Procedure:** How to Copy and Paste an Access Control Template

1. On the WebFOCUS Client, navigate to the `drive:\ibi\profiles` directory.
2. Open the file `admin.cfg` with a text editor.

3. Scroll down to the line:

```
[Access Control]
authenticate_all_pthuser = y
prepend_provider_name = n
```

4. Copy the following text and paste it after the last statement in the admin\_level = OPR section and before the title [Access Control].

```
admin_group = Administrators
BEGIN
    admin_level = SRV
    admin_description = WebFOCUS Administrators
END
admin_group = Managers
BEGIN
    admin_level = SRV
    admin_description = WebFOCUS Managers
END
admin_group = modelgrp/Developers
BEGIN
    admin_level = APP
    admin_privilege = *;ANONE
    admin_privilege = (APPROOT)/baseapp;AREAD,PRRUN,ALIST
    admin_privilege = (APPROOT)/modelapp;AREAD,ARWRT,PRRUN,ALIST
    admin_privilege = (APPROOT);ANONE
    admin_privilege = ADPTP,NODPT,NOSYS,METAP,DATMG,PRSAV,PRDFR,
        PRRPT,PROUT,MONIT,SRVLG,KILT3,APATH
    admin_privilege = (APPROOT)/ibisamp;AREAD,PRRUN,ALIST
END
admin_group = modelgrp
BEGIN
    admin_level = USR
    admin_privilege = NODPT,NOSYS,PRDFR,PRRPT,PROUT,KILT3,APATH
    admin_privilege = *;ANONE
    admin_privilege = (APPROOT)/baseapp;AREAD,PRRUN,ALIST
    admin_privilege = (APPROOT)/modelapp;AREAD,PRRUN,ALIST
    admin_privilege = (APPROOT);ANONE
    admin_privilege = (APPROOT)/ibisamp;AREAD,PRRUN,ALIST
END
admin_group_template = (.+)/Developers
BEGIN
    model_group = modelgrp/Developers
    file_replace_pattern = (modelapp)
END
admin_group_template = (.+)
BEGIN
    model_group = modelgrp
    file_replace_pattern = (modelapp)
    exclude_groups = (/)
END
```

5. Optional: If users do not need to access the ibisamp or baseapp application directories, delete the lines pertaining to them from the admin\_group = modelgrp and admin\_group = modelgrp/Developers sections of the Application Control section text.

6. Save and close the admin.cfg file.

Continue the configuration by limiting the range of available resources, if necessary. You can then test the entire solution as described in the topic, [Testing the Combined Resource Template and Access Control Template Solution](#) on page 433.

## Creating Access Control Templates by Manual Configuration

The manual method of creating an access control template requires an administrator to use the Reporting Server browser interface to create a template model and then register access control templates based on that model. When the template model is configured, the administrator registers individual templates based on it to groups. The registration identifies the access control template to use when users from a specific group deliver a request to the WebFOCUS Reporting Server through a trusted connection.

### Creating a Template Model

A template model represents the configuration of groups that can connect to the WebFOCUS Reporting Server and the privileges those groups can maintain. It incorporates your access control policy directly into WebFOCUS Reporting Server settings.

To create a template model:

1. Create an Administrators group and register it to the Server Administrators Role on the WebFOCUS Reporting Server.
2. Create a Managers group and register it to the Server Administrators Role on the WebFOCUS Reporting Server.
3. Create a model application.
4. Create a model group and register it to the Basic Users Role.
5. Create a model/developers group and register it to the Application Administrator Role.

The Administrator and Managers groups enable anyone in the Administrators group, as well as the Managers group, to access the WebFOCUS Reporting Server and Reporting Server browser interface with single sign on as a Server Administrator.

The model group and model developers group represent workspace groups. They enable users in workspace sub-groups to connect to the WebFOCUS Reporting Server as a user or developer with single sign on access. The model application represents application folders that users who are connected to the WebFOCUS Reporting Server through the trusted connection can create. As described in these topics, this template model applies the familiar default configuration of permissions. However, the Reporting Server browser interface gives administrators the tools to create any kind of access control template that conforms to the security requirements of their installation.

### ***Procedure:*** How to Sign in to the WebFOCUS Reporting Server Browser Interface

To be able to open, review, and update group privileges, ensure that the WebFOCUS Reporting Server is running in the Security On mode before you begin the access control template configuration.

1. Sign in as an administrator.
2. On the Hub, select *Management Center* and *Access Control* from the side navigation pane.

Or

Open the WebFOCUS Home Page, and select *Settings* and *WebFOCUS Server*.

Or

Open the *Plus* menu and then select *Prepare and Manage Data*.

Or

Type the following URL in the browser address bar:

`http(s)://host:port/context/admin`

where:

`host`

Is the name or IP address of the host used to access WebFOCUS.

`port`

Is the number of the port on which the WebFOCUS Reporting Server or Application Server listens.

This value is optional, and it should be excluded if the URL uses the default port for the protocol it uses in the scheme, which is port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

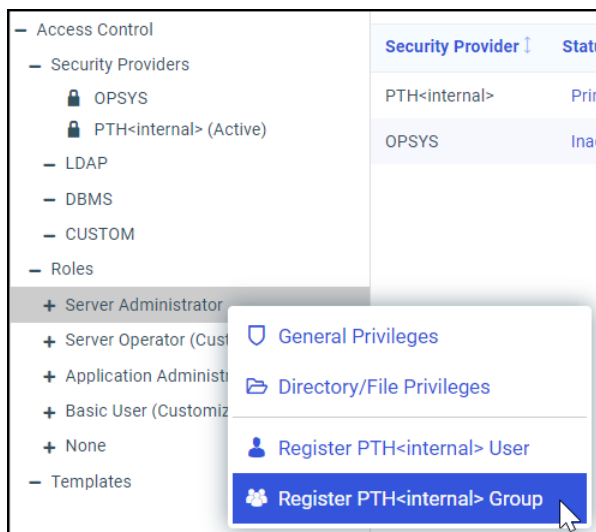
`context`

Is the specific context used for WebFOCUS. For example, *ibi\_apps*.

**Note:** If you are signed in, and the machine id, port, and context already appear in the address bar, you only need to type over that part of the path that follows the context with the term `/admin`.

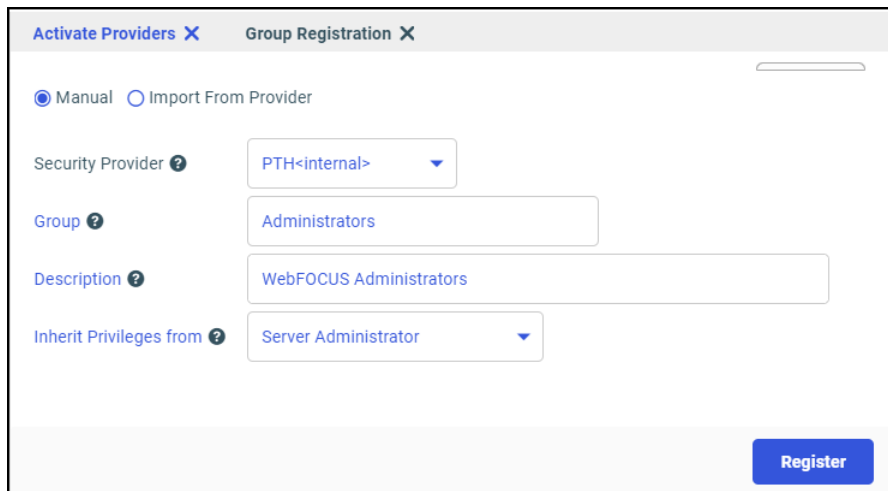
**Procedure:** How to Create and Register the WebFOCUS Administrators and Managers Groups to the Server Administration Role

1. Open the Reporting Server browser interface, select *Settings*, and then select *Access Control*.
2. In the Access Control tree, under the Roles folder, right-click *Server Administrator*, and then click *Register PTH <Internal> Group*, as shown in the following image.



3. On the Group Registration tab, click *Manual*.

4. When the Group Registration tab refreshes, type *Administrators* in the Group field, type *WebFOCUS Administrators* in the Description field, and then click *Register*, as shown in the following image.



Activate Providers X Group Registration X

☒ Manual ☐ Import From Provider

Security Provider ? PTH<internal>

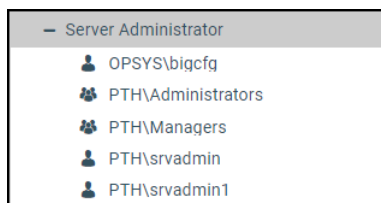
Group ? Administrators

Description ? WebFOCUS Administrators

Inherit Privileges from ? Server Administrator

Register

5. When you receive a confirmation message, click *OK*.  
The Reporting Server browser interface screen refreshes.
6. Repeat steps 2 through 5 to create and register a second group to the Server Administrator role, but this time, type *Managers* in the Group field, and then type *WebFOCUS Managers* in the Description field.
7. After you have created and registered the second group, under the Roles folder, expand the Server Administrator role and ensure that the new groups appear under it, as shown in the following image.



These two groups enable anyone in the WebFOCUS Administrators group, as well as the WebFOCUS Managers group, to use a single sign-on to access the WebFOCUS Reporting Server and Reporting Server browser interface as a Server Administrator.

**Note:** The product installation automatically adds the OPSYS\IBI\username and PTH\srvadmin users that appear under the Server Administrator role.



### **Procedure: How to Create and Register the Modelapp Application**

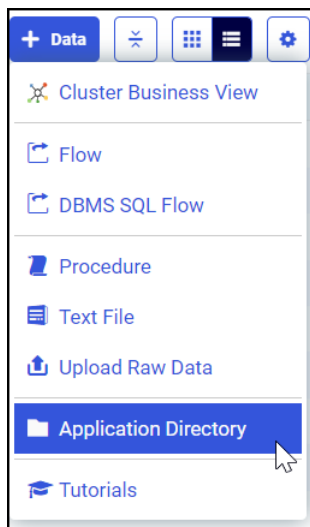
The modelapp application is a placeholder for all applications and application directories assigned to workspaces on the WebFOCUS Reporting Server.

1. On the Hub, in the left navigation pane, select *Application Directories* to open the Application Directories area.

Or

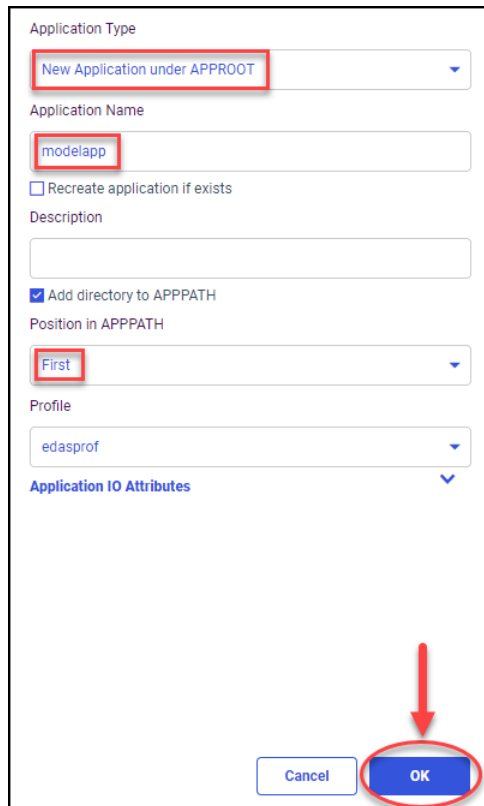
Open the Reporting Server browser interface. The Applications area appears, by default.

2. Select *Data* and *Application Directory*, as shown in the following image.



3. On the Create New Application tab, perform the following steps:
  - a. Ensure that the value *New Application under APPROOT* appears in the Application type field.
  - b. Type *modelapp* in the Application Name field.

- c. Click *First* in the Position in APPATH list, as shown in the following image, and then click *OK*.

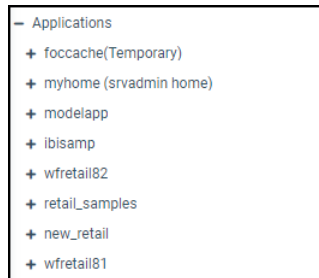


The screenshot shows a configuration window with the following fields and controls:

- Application Type:** A dropdown menu with "New Application under APPROOT" selected. This field is highlighted with a red rectangle.
- Application Name:** A text input field containing "modelapp". This field is highlighted with a red rectangle.
- Recreate application if exists:** An unchecked checkbox.
- Description:** An empty text input field.
- Add directory to APPATH:** A checked checkbox.
- Position in APPATH:** A dropdown menu with "First" selected. This field is highlighted with a red rectangle.
- Profile:** A dropdown menu with "edasprof" selected.
- Application IO Attributes:** A section header with a downward arrow.
- Buttons:** "Cancel" and "OK" buttons at the bottom right. The "OK" button is circled in red, and a red arrow points down to it.

The Reporting Server browser interface refreshes the screen, and displays the Status page.

The folder for the new sub-application appears under the Application Directories folder, as shown in the following image.



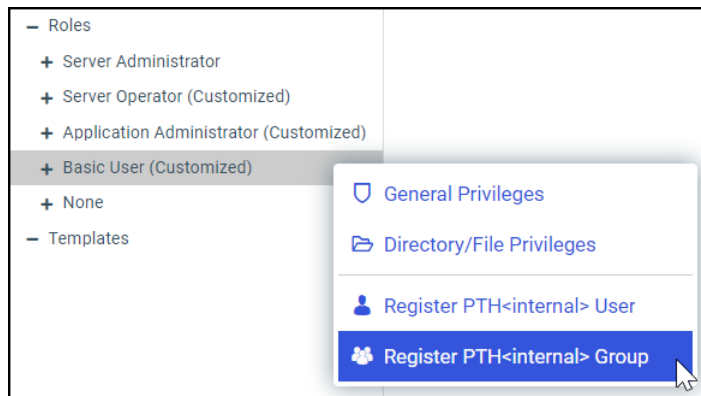
### **Procedure:** How to Register the New Group, ModelGrp

1. Perform one of the following steps to open the Access Control View.

On the Hub, in the left navigation pane, select *Management Center* and *Access Control*.

Navigate to the Reporting Server browser interface, select *Tools*, and then select *Access Control*.

2. In the Access Control tree, under the Roles folder, right-click the *Basic User* role, and then click *Register PTH<internal>Group*, as shown in the following image.



3. On the Group Registration tab, click *Manual*.

- When the tab refreshes, in the Group field, type *modelgrp*, and then click *Register*, as shown in the following image.

The screenshot shows the 'Group Registration' tab with the 'Manual' radio button selected. The 'Security Provider' dropdown is set to 'PTH<internal>'. The 'Group' text field contains 'modelgrp'. The 'Description' text field is empty. The 'Inherit Privileges from' dropdown is set to 'Basic User'. A blue 'Register' button is located at the bottom right of the form.

- When you receive a message that a new group will be registered, click *OK*.
- In the Access Control Tree, under the Roles folder, right-click the *Application Administrator* role, and then click *Register Group*.
- On the Group Registration page, click *Manual*.
- When the page refreshes, type *modelgrp/Developers* in the Group field, and then click *Register*, as shown in the following image.

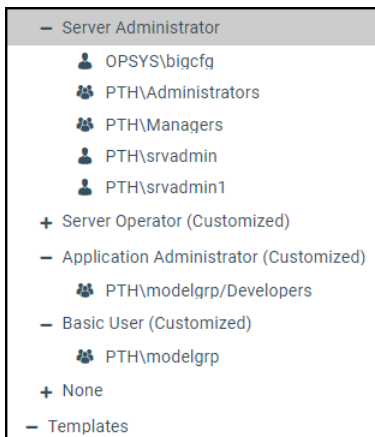
The screenshot shows the 'Group Registration' tab with the 'Manual' radio button selected. The 'Security Provider' dropdown is set to 'PTH<internal>'. The 'Group' text field contains 'modelgrp/Developers'. The 'Description' text field is empty. The 'Inherit Privileges from' dropdown is set to 'Application Administrator'. A blue 'Register' button is located at the bottom right of the form.

- When you receive a message that a new group will be registered, click *OK*.

The Reporting Server browser interface displays the Activate Providers list.

10. In the Access Control Tree, under the Roles folder, expand the *Application Administrator* and *Basic User* roles.

Icons for the Administrators and the Managers Groups appear under the Server Administrator role. An icon for the modelgrp/Developers group appears under the Application Administrator role, and an icon for the modelgrp appears under the Basic User role, as shown in the following image.



**Important:** Before continuing, review the spelling and capitalization of the names of the users and groups you just registered. Group names are case-sensitive on the WebFOCUS Reporting Server. Therefore, you must spell and capitalize modelgrp/Developers exactly as shown in these examples, including the uppercase D.

### **Procedure:** How to Configure Group Privilege Assignments

1. Perform one of the following steps to navigate to the Application Directories page.

On the Hub, in the left navigation pane, select Application Directories.

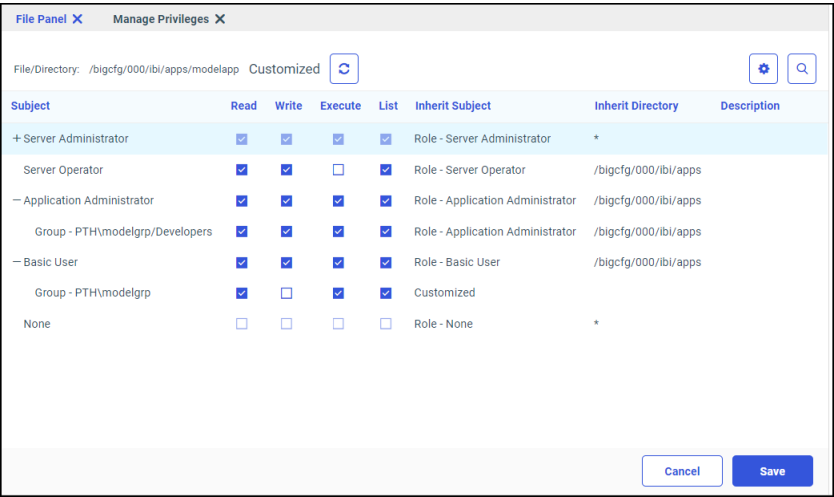
Or

Navigate to the Reporting Server browser interface. The Applications page opens, by default.

2. Right-click *modelapp*, and then click *Privileges*.
3. On the Manage Privileges page, in the Subject column of the Customized list:
  - a. Under Application Administrator, in the Group - modelgrp/Developers entry, ensure that the *Read*, *Write*, *Execute*, and *List* check boxes are selected.

- b. Under Basic User, in the Group - PTH\modelgrp entry, ensure that the *Read*, *Execute*, and *List* check boxes are selected. Clear the *Write* check box if it is not cleared, by default.

Review the page to ensure that seven (7) checkmarks are defined on the rows, as shown in the following image.



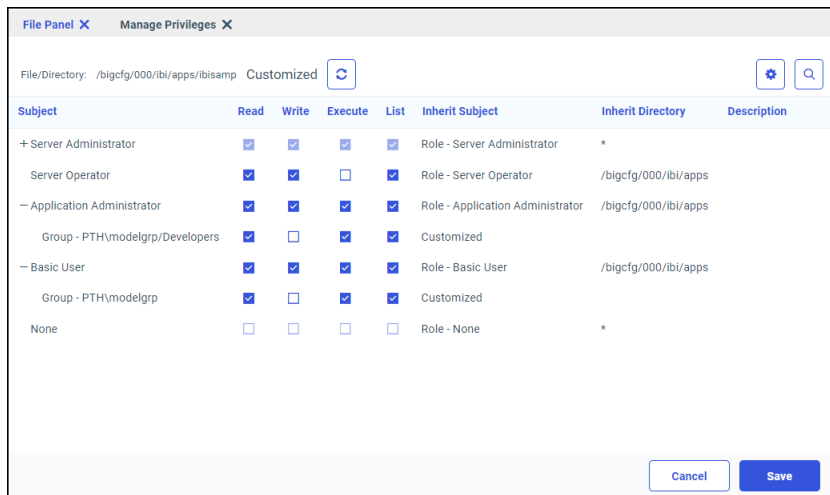
This configuration conforms to the business requirements stated in the topic [Developing Business Requirements for Server Access Control Templates](#) on page 402. Developers have read/write access to their application, and Basic and Advanced users have read only access to their application.

**Note:** If you were required to select or clear any of these check boxes to ensure that they conform to this configuration, click Save.

**Procedure: How to Review Permissions Assigned to the ibisamp and baseapp Application**

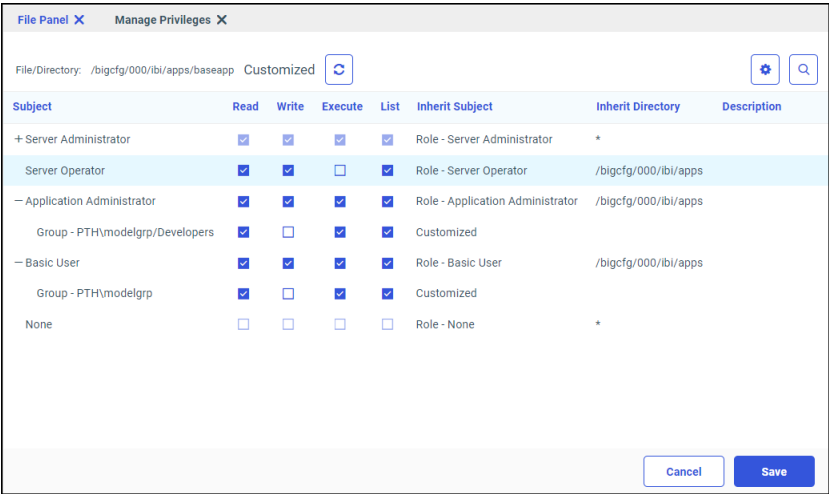
1. In the Reporting Server browser interface, on the Applications tab, under the Applications folder, right-click the *ibisamp* folder, and then click *Privileges*.
2. On the Manage Privileges page, in the Customized list Subject column:
  - a. Under Application Administrator, in the Group - PTH\modelgrp/Developers entry, ensure that the *Read*, *Execute*, and *List* check boxes are selected. Ensure that the *Write* check box is cleared.

- b. Under Basic User, in the Group - PTH\modelgrp entry, ensure that the *Read*, *Execute*, and *List* check boxes are selected. Ensure that the *Write* check box is cleared, as shown in the following image.



3. On the Applications tab, under the Applications folder, right-click the *baseapp* folder, and then click *Privileges*.
4. On the Manage Privileges page, in the Customized list Subject column:
  - a. Under *Application Administrator*, in the Group - PTH\modelgrp/Developers entry, ensure that the *Read*, *Execute*, and *List* check boxes are selected. Ensure that the *Write* check box is cleared.

- b. Under *Basic User*, in the Group - PTH\modelgrp entry, ensure that the *Read*, *Execute*, and *List* check boxes are selected. Ensure that the *Write* check box is cleared, as shown in the following image.



**Note:** To update these settings to conform to your requirements, you can also clear the Read/Write/Execute and List privileges for the modelgrp/Developers and modelgrp Roles.

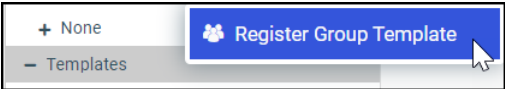
Creating and Registering Server Access Control Templates

Access control templates dynamically apply the access control policies defined on the *modelapp* applications to every connection.

To create a server access control template, identify the range of groups to which the template will be applied dynamically.

Procedure: How to Create and Register the modelgrp/developers Access Control Template

1. On the Reporting Server browser interface, select *Tools*, and then select *Access Control*.
2. Right-click the *Templates* folder, and then click *Register Group Template*, as shown in the following image.



3. On the Group Template Registration page, in the Template Group ID field, type, (.+)/*Developers*.



This value identifies the template on the tree and also defines the pattern matching logic that will be associated with this template. In this case, the template defines a connection to the server that is accompanied by a group whose name follows the convention, *<Group>/Developers*.

This value identifies the privileges automatically assigned to the Developers sub-group of any workspace group created after this access control template is activated.

4. Click *modelgrp/Developers* in the Model Group list.

Connections matched to this template are assigned the access privileges of this group.

5. Bypass the Exclude Group IDs field.
6. In the Replace Pattern field, type (*modelapp*).

This value specifies that access privileges assigned to the modelapp group will be assigned to any basic user group whose name fits the modelapp pattern.

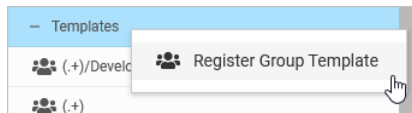
**Note:** When the WebFOCUS Reporting Server runs on Windows, the directory delimiter is a backslash (\). Therefore, you are required to escape each backslash with an additional backslash. For example, (\\).

7. Confirm that you have typed the correct settings.
8. Click *Register*.

The Group Template Registration page refreshes and an entry for the template appears underneath the *Templates* node on the Access Control page.

### **Procedure:** How to Create and Register the modelgrp Access Control Template

1. On the Access Control tab, right-click the *Templates* node, and then click *Register Group Template*, as shown in the following image.



2. In the Template Group ID field, type, (.+).

This value identifies the privileges automatically assigned to the Basic User and Advanced User sub-groups of any workspace group created after this access control template is activated.

3. Click *modelgrp* in the Model Group list.

Connections matched to this template are assigned the access privileges of this group.

4. Type (/) in the Exclude Group IDs field.

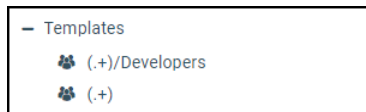
This value helps prevent groups whose name uses the anygroup/GroupName format from being assigned to the (.+) template.

5. In the Replace Pattern field, type (*modelapp*).

This value specifies that the dynamically assigned access privileges will be switched from (*modelapp*) to the name of the trusted group. For example, (*modelapp*) will be replaced with *sales* for users in the *sales\advancedusers* group.

6. Confirm that you have typed the correct settings.
7. Click *Register*.

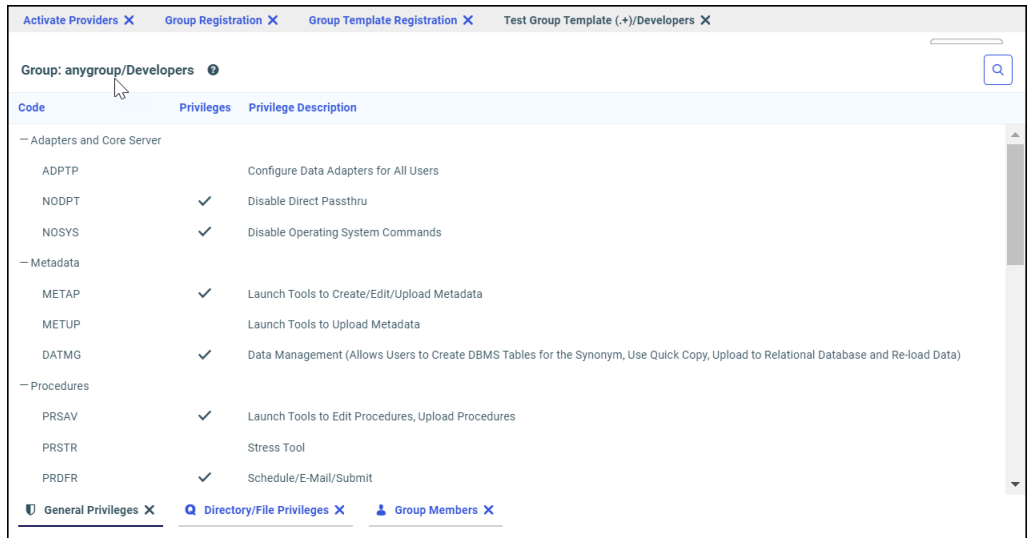
Entries for both templates appear underneath the Templates node on the Access Control page.



### ***Procedure:*** How to Test the modelgrp and modelgrp/developers Access Control Templates

1. In the Reporting Server browser interface, on the Access Control tab, under the Templates folder, right-click the template (.+)/Developers, and then click *Test*.
2. In the Group ID field, type *anygroup/Developers*, and then click *Next*.

The Test Results window opens, displaying the General Privilege page with the name of the group typed in the Group ID field, as shown in the following image.



The list of general privileges demonstrates that anyone belonging to a group with a name that conforms to the pattern *anygroup/Developers* will be associated with the modelgrp/Developers server role, as expected.

3. Click the Directory/File Privileges tab.

The Directory/File Privileges list shows that the expected access privileges are defined for members of the *anygroup/Developers* group. Specifically, it shows those privileges on the *anygroup* application folder that are assigned to any workspace group to which the user belongs.

Activate Providers X Group Registration X Group Template Registration X Test Group Template (-+)/Developers X

Group: anygroup/Developers

Directory/File	Read	Write	Execute	List	Status	Inherit Subject	Inherit Directory
- *	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Inherited	Role - Application Administrator	*
- /	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Inherited	Role - Application Administrator	*
- bigcfg	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Inherited	Role - Application Administrator	*
- 000	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Inherited	Role - Application Administrator	*
- ibi	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Inherited	Role - Application Administrator	*
- apps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inherited	Role - Application Administrator	/bigcfg/000/ibi/apps
baseapp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	System Default		
ibisamp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	System Default		
- homeapps	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	System Default		
<user>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	System Default		
- profiles	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	System Default		
<user>.prf	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	System Default		

General Privileges X Directory/File Privileges X Group Members X

Even though the *anygroup* application does not yet exist, the access control template defines the privileges and role assignments attached to any incoming request that matches this particular template.

**Procedure:** How to Restart the WebFOCUS Reporting Server

You must restart the WebFOCUS Reporting Server after adding or updating access control templates to make the new or updated templates available to future connections.

- 1. On the Reporting Server browser interface, open the Workspace tab.
- 2. In the Operations group, click *Restart*.
- 3. When you receive a confirmation message, click *OK*.

The Reporting Server browser interface displays a message indicating that the Workspace is restarting.

- 4. When the Reporting Server browser interface refreshes and returns you to the Applications tab, close the Reporting Server browser interface.

Continue the Reporting Server browser interface configuration by limiting the range of available resources, if necessary. You can then test the entire solution as described in the topic, [Testing the Combined Resource Template and Access Control Template Solution](#) on page 433.

## Testing the Combined Resource Template and Access Control Template Solution

Tests of the resource template and access control template solution help you ensure that new workspaces and groups maintain a level of access that conforms to your original design. By creating new workspaces and new users, and then assigning them to workspace groups, you can test the range of features provided to users. You can ensure that the privileges assigned to new users and groups match the expected range of capabilities, and that they conform to the requirements and responsibilities of users in their group.

To test the combined solution:

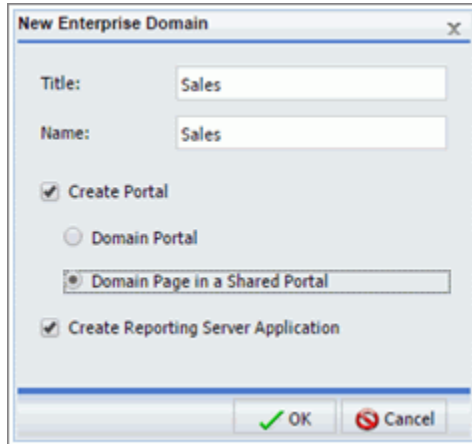
- ☐ Sign in as a member of the Administrator group, and create two workspaces that include the Workspace Portal and WebFOCUS Reporting Server Applications options.
- ☐ For each workspace, create a user and assign that user to the Advanced Users group of that workspace.
- ☐ For each workspace, create a second user and assign that user to the Developers group of that workspace.
- ☐ Sign in as an advanced user, and ensure that you can see or run content in the workspace to which you are assigned, and in the other workspaces that have been made accessible to all advanced users.
- ☐ Sign in as a developer, and ensure that you can see, run, and create content in the workspace to which you are assigned, and in the other workspaces that have been made accessible to developers.

### **Procedure:** How to Create Workspaces for the Access Control and Resource Template Solution Test

This feature is only available from the Legacy Home Page.

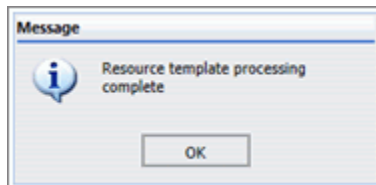
1. Sign in as an administrator.
2. Open the Legacy Home Page.
3. In the Resources tree, right-click the *Workspaces* node, point to *New*, and then click *Enterprise Workspace*.

4. In the New Enterprise Workspace dialog box, select the *Create Portal* check box, select the *Domain Page in Shared Portal* option, and then select the *Create Reporting Server Application* check box.
5. In the Title field, type *Sales*. The same value is assigned to the Name field automatically, as shown in the following image.

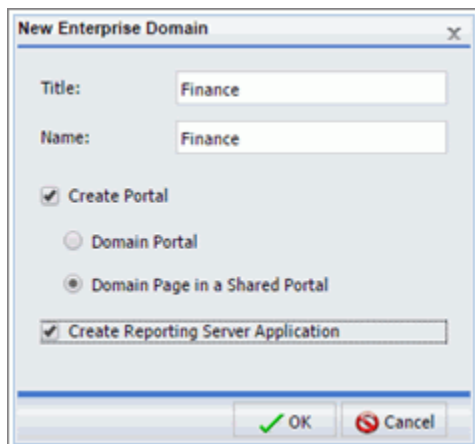


In this example, the resource template was designed to create tenant applications through the WebFOCUS Client node named *EDASERVE*. This node must be configured to point to the WebFOCUS Reporting Server with the access control template you just created and the WebFOCUS Reporting Server it points to must be running when you conduct this test.

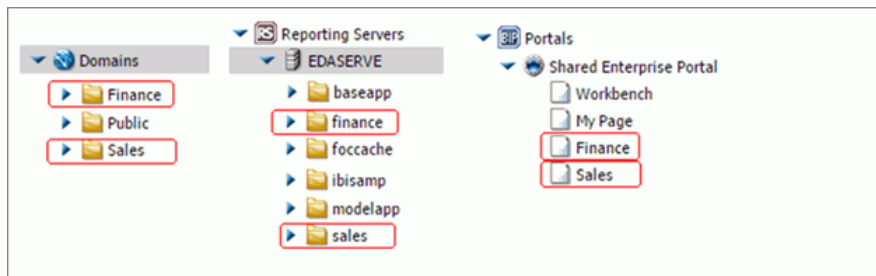
6. Click *OK*.
7. When you receive the Resource template processing complete message, click *OK*, as shown in the following image.



8. Repeat steps 2 through 6 to create another workspace. For this second workspace, type *Finance* in the Title field, as shown in the following image



9. Ensure that folders for the Finance and Sales workspaces appear on the Resources tree, under the Workspaces node, under the Reporting Servers node, and under the Portals node, as shown in the following image.



**Procedure: How to Create Users for the Access Control and Resource Template Solution Test**

1. Open the Security Center.
2. In the Users pane, click *New User*.
3. Type *fdev*, in the User Name field.
4. Click *Finance/Developers* in the Create in Group list.
5. Click *OK*.
6. Repeat steps 2 though 5 to create another user. For this second user, type *sdev* in the User Name field, and click *Sales/Developers* in the Create in Group list.
7. When you are finished, exit the Security Center, and sign out.

**Procedure: How to Add Metadata to the Test Workspaces**

This topic calls for you to copy the *car.foc* file from the *ibisamp* application folder and paste it into the application directories of your new workspaces. However, you can substitute any metadata file for the *car.foc* file to conduct this test.

This feature is only available from the Legacy Home Page.

1. Open the Legacy Home Page.
2. In the Resources tree, expand the *Reporting Servers* node, and then expand the *EDASERVE* node.
3. Expand the *ibisamp* folder, right-click *car.foc*, and then click *Copy*.
4. Under the *EDASERVE* node, right-click the *finance* folder, and then click *Paste*.
5. Rename the *car.foc* file to *finance.foc*.
6. In the *ibisamp* folder, right-click *Legacy Metadata Sample: car.mas*, and then click *Copy*.
7. Right-click the *finance* folder, and then click *Paste*.
8. Repeat steps 2 through 6. This time copy the *car.foc* and *Legacy Metadata Sample: Car.mas* files to the *Sales* folder under the *EDASERVE* node.

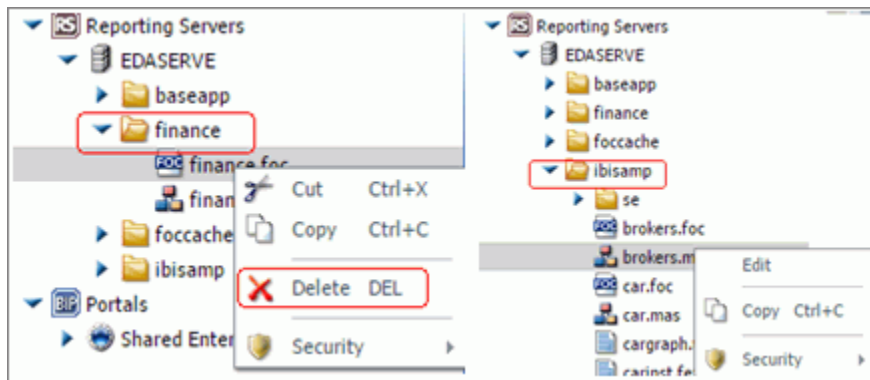
**Procedure: How to Test the Privileges of a Workspace Developer Group Member**

This feature is only available from the Legacy Home Page.

1. Sign out, and sign in with the *fdev* User Name.
2. Open the Legacy Home Page.
3. In the Resources tree, expand the *Reporting Servers* node.
4. Expand the *EDASERVE* node, and ensure that the *finance* application folder appears.
5. If you gave this workspace developer group Read, Execute, and List privileges for the *ibisamp* and *baseapp* application directories, ensure that these two folders also appear under the *EDASERVE* node.
6. Right-click the *finance* folder, and review the shortcut menu. Determine if the *Delete* command appears.



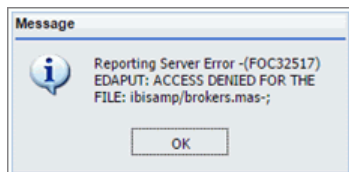
7. Right-click the *ibisamp* or *baseapp* application folder, and review the shortcut menu. Compare the list of available commands to those on the *finance* folder shortcut menu, as shown in the following image.



Notice that WebFOCUS knows that the *fdev* user does not have Write privileges on the *ibisamp* application so the *Delete* command is not available on the shortcut menu for these folders. The access control templates dynamically assign privileges to the folders according to the privileges defined in the template.

However, notice that the *Edit* command is available on the shortcut menu for the *Legacy Metadata Sample: brokers.mas* file in the *ibisamp* folder.

8. Right-click the *Legacy metadata Sample: brokers.mas* node under the *ibisamp* folder, and then click *Edit*.
9. Make some edits to the file, and then click *Save*.
10. If you receive a message from the WebFOCUS Reporting Server, as shown in the following image, click *OK*.



This message indicates that the *fdev* user does not have sufficient access privileges on the WebFOCUS Reporting Server to edit the file.

The *Edit* command appears in the shortcut menu for the folder because, in the Resources tree, the *Edit* command is synonymous with the *Open* command. As in other software systems, the *Edit* command is used for both viewing and editing.

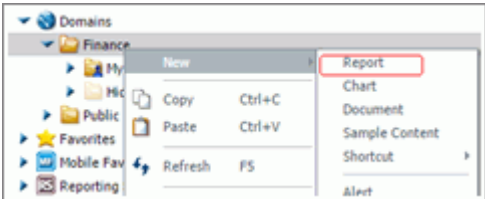
11. Close the Editor.

12. When you receive a message asking to save your changes, click No.

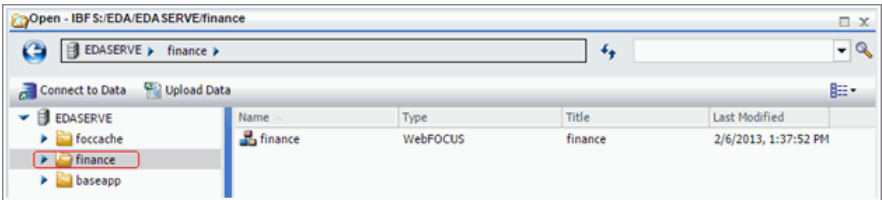
**Procedure: How to Test the Range of Folders Accessible to a Workspace Developer Group Member**

This feature is only available from the Legacy Home Page.

- 1. Open the Legacy Home Page.
- 2. In the Resources Tree, under the Workspaces node, right-click the *Finance* folder, point to New, and then click *Report* as shown in the following image.



The Open dialog box displays the finance application directory folder as the default application, as shown in the following image.




The foccache and baseapp application directory folders are special cases, and the Open dialog box will always display them, if the access control template assigned to the WebFOCUS allows the user to list those applications. Although this user in the Developer group has access to ibisamp application, it is not shown within InfoAssist, because that application is not part of the application path when the Workspace was created with the Enterprise Resource Template.

You can add Descriptions to your MFDs with the DESCRIPTION keyword, as shown in the following example for the *finance* Master File:

```
FILENAME=WMDATA,DESCRIPTION='Finance Data',SUFFIX=FOC
```

```
SEGNAME=ORIGIN,SEGTYPE=S1
```

- 3. Click *Cancel*  to close the Open dialog box without creating a report.

4. Close the InfoAssist window.

### Assess Your Test Results

If one or more of these tests did not produce the expected results, return to the access control template configuration topics and address the issue. However, if the results of the tests conform to expected behavior, you can confirm that your access control template and resource template solution is ready for implementation.

## Working With Message Templates

Message templates that define user interface objects, such as the Deferred Reporting interface, and the messages they display, are stored as separate xml files in the prod directory, located in `drive:\ibi\WebFOCUS\client\wfc\etc\`, and are now available for customization.

Custom message templates are based on standard message templates, but can contain specialized text, images, and layouts that conform to the requirements of a local product installation. Multiple language versions of custom message templates ensure that the same customized information is available to all users, regardless of the language they use in daily operations. When used in place of a standard message template, custom message templates enable a local installation to display localized text and branding.

To activate the use of a custom message template, administrators copy a standard message template, paste it into the custom directory, located in `drive:\ibi\WebFOCUS\client\wfc\etc\`, and adapt that copy to their requirements. Once established in the custom directory, the custom message template is retrieved automatically, instead of the standard message template. If there is no message template in the custom directory, the standard message template from the prod directory is used instead.

Custom message templates remain unchanged during the upgrade process, preserving the time and effort spent to develop them. A separate utility enables administrators to review custom message templates after an upgrade and ensure that they remain intact.

The text displayed within objects created by templates can be customized as well. Using the `webfocus-intl.jar` file, located in `drive:\ibi\WebFOCUS82\webapps\webfocus\WEB-INF\lib`, administrators create custom copies of standard message text strings.

Administrators can also create multiple language versions of custom message strings, to ensure that the same customized text is available to all users, regardless of the language they use in daily operations.

### Procedure: How to Create Custom Message Templates

Custom message templates are based on previously-created prod templates. To produce a custom message template, copy the standard message template on which it is based from the prod directory to the custom directory. This operation does not require the use of the Administration Console or other user interface.

1. On a machine running the WebFOCUS Client, open the prod directory, located in *drive:\ibi\WebFOCUS\client\wfc\etc\prod*.
2. Right-click the template that you want to customize, and then click *Copy*.
3. Open the custom directory, located in *drive:\ibi\WebFOCUS\client\wfc\etc\custom*, and then click *Paste*.

**Note:** Do not change the template name.

### Understanding Message Template Text Strings

Messages are produced by merging text strings stored in a separate file into a message template that corresponds to the number of the system event or error. For example, when the WebFOCUS Reporting Server generates error 42, the message template for error 42 is invoked and populated with text strings that are identified within the error 42 template, as shown in the following image.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 1996-2015 Information Builders, Inc. All rights reserved. -->
<!--$Revision: 1.1 $:-->
<templates>
  <template name='error_42'>
    <![CDATA[
      <HTML>
      <HEAD>
      <TITLE><inserttext err_42 /></TITLE>
      </Head>
      <Body>
      <HR><H3>
      <inserttext err_42_explain1 /><p>
      <inserttext err_42_explain2 /><br>
      <inserttext err_42_explain3 /><br>
      <inserttext err_42_explain4 /><br>
      <inserttext err_42_explain5 />
      </H3><HR>
      <PRE>
      <H5>
      <insertvariable html_no_output_msg />
      </H5>
      </PRE>
      </Body>
      </HTML>
    ]]>
  </template>
</templates>
```

The links in the inserttext tags in this example connect to the localization files that contain the text displayed in the message. If customization of this text is necessary, please contact Customer Support.



## User Administration

---

This topic explains how to manage users, groups, roles, and rules. These functions can be performed by a user with full administrative privileges, but you can also delegate a limited subset of administrative privileges to subadministrators. Functions which are frequently delegated include:

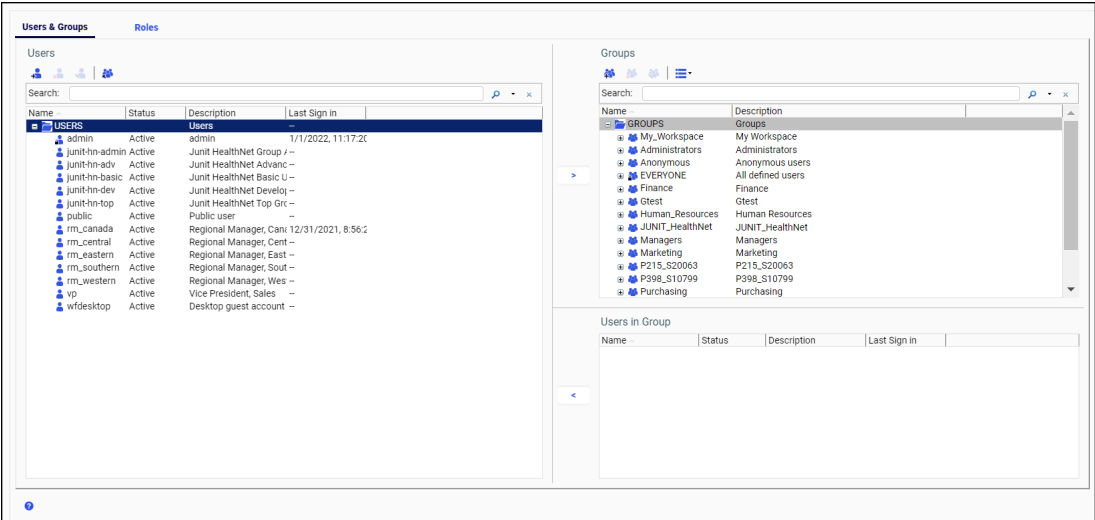
- ☐ Creating groups and users.
- ☐ Assigning users to groups.
- ☐ Creating limited security rules, such as denying members of a special group access to a subfolder.
- ☐ Managing private content for users.
- ☐ Reassigning ownership of resources, such as schedules or reports.

**In this chapter:**

- ☐ [Using the Security Center](#)
  - ☐ [Managing Users](#)
  - ☐ [Managing Groups](#)
  - ☐ [Managing Roles](#)
  - ☐ [Managing Rules](#)
  - ☐ [Managing Private Resources](#)
-

## Using the Security Center

You can use the Security Center to manage and make rules on users, groups, and roles. To launch the Security Center from the Hub side navigation pane, select *Management Center* and *Security Center*. From the WebFOCUS Home Page, select *Settings* and *Security Center* from the Banner on the WebFOCUS Home Page. The Security Center appears, as shown in the following image.



## Managing Users

The Users field in the Users & Groups tab of the Security Center lists all users in the repository. The Search field in this tab allows you to search the name and description fields for users. Simple wildcard searches are supported. A toolbar allows you to perform the following actions:

- ☐ Create, edit, or delete users.
- ☐ Import users.
- ☐ View or edit the access rules on a group.
- ☐ View when users last signed in.



## Understanding Users

Users are those individuals who have access to WebFOCUS. Administrators and Group Administrators can assign users with similar responsibilities to one of the user type groups that are automatically created within a workspace. This assignment allows users to take advantage of those features and content that supports their daily activities, but prevents them from using features or content that are beyond the range of their responsibilities and authority. Administrators can adapt groups and the features and content they make available to the unique requirements of their product installation. In general, however, the four groups grant the following privileges to the users assigned to them:

- ❑ **Basic Users.** Can view reports and content in the workspaces accessible to them. They can save deferred reports to their My Content folders, or copy parameters from a previously created report. They cannot share, publish, copy, or paste any folder or content.
- ❑ **Advanced Users.** Can do everything that Basic Users can do, and can also create original reports, charts and other content for their My Content folders. They can share folders and the content they contain with everyone or with selected users or groups.
- ❑ **Developers.** Can do everything that Advanced Users can do, and can view and publish content in their Hidden Folder. They can also copy and paste folders and content from their workspace to another workspace, but they must be sure that the workspace they target for this operation maintains the same metadata as that used to create the content they are copying.
- ❑ **Group Administrators.** Can assign users to groups. They can also switch to Administrator Mode and manage private resources. SaaS and Enterprise Group Administrators can add or remove available users to or from the groups they manage. The DomainGroupAdminScope rule limits the range of users that are visible to SaaS Group Administrators to those users assigned to their tenant group. Enterprise Group Administrators can also create new users and can delete or edit the accounts of users who are in their parent group. Neither SaaS nor Enterprise Group Administrators can run reports unless they are also assigned to another group, such as BasicUsers.

Each user in the Repository is defined by a unique name, and may also be assigned a description, an email address, and a password. The user must be placed in a group at account creation and assigned a status. By default, a new user is placed in the EVERYONE group, which is the group of all users in the system, and assigned the Active status.

Any of these characteristics, except the unique username, may be edited later by an administrator.

## Understanding User Name Requirements

Because user names are defined within the Repository, they need to conform to the format rules and character limitations it imposes. If your installation supports external authentication, such as that provided by Microsoft Active Directory, user names also exist in an external repository, and must conform to the format rules defined within it.

The set of characters you can use to create user names is defined by the current character encoding setting established in the application server and the Client Code pages assigned to your NLS setting. For example, if the application server is configured to support UTF-8 encoding, and the NLS Setting is also configured to support the US Unicode (UTF) code page, you can use characters in the double-byte character set (DBCS) to create user names.

To support those installations that rely on external LDAP or Active Directory authentication, WebFOCUS user names support all of the characters supported by the sAMAccountName standard. Note that the range of allowable characters for User Names in WebFOCUS is broader than the range for the sAMAccountName standard, and administrators must be careful to avoid including characters allowed by WebFOCUS but prohibited by the sAMAccountName standard in User Names.

Given these considerations, when creating user names, take the following rules into account:

- ☐ User names may contain alphanumeric characters, spaces, and underscores.
- ☐ Depending upon the Client Code Page assigned to your NLS setting, user names can also include single-byte or double-byte NLS characters.

**Note:** To prevent sign-in issues, and to conform to sAMAccountName best practices, replace characters that contain accents or other diacritical marks in user names with characters that exclude them. For example, convert Müller into Muller.


- ☐ The following characters are not supported in user names : " | ; / \* , ?

**Note:** if your user names must conform to sAMAccountName standards, you must independently ensure that user names also exclude the following characters: [ ] : = + < > \

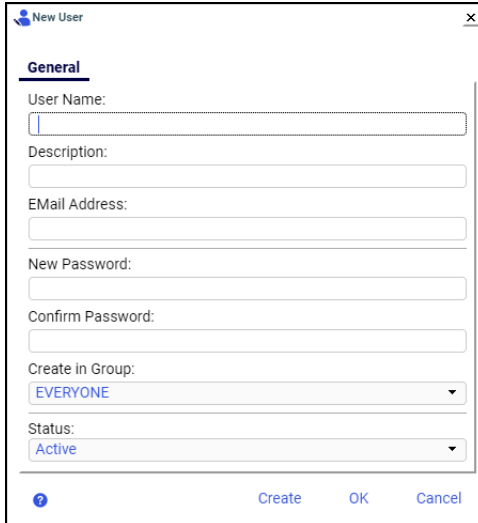
- ☐ It is recommended that you limit user names to 255 characters. Longer user names may cause problems during migration.
- ☐ Do not end user names with a period (.).

If you support external authentication, avoid including characters in user names that your external authentication repository does not support. For more information about which characters to avoid, contact Customer Support Services.

### Procedure: How to Create a User

1. In the Security Center, on the Users & Groups tab, click the *New User* button .

The New User dialog box opens, as shown in the following image.



**Note:** The New Password and Confirm Password fields do not appear in the New User dialog box if your organization has enabled external security and assigned user authentication to a WebFOCUS Reporting Server that does not require passwords to open user accounts.

2. Type the user name, and optionally, type the description, email address, password, and password confirmation, and if desired, select a group and a status for the user.
3. When your input is complete:

- a. Click *OK* to create the user and close the New User dialog box.
- b. Click *Create* to create the user without closing the New User dialog box.

Use this button when you need to create additional users without delay. When you click this button, the New User dialog box clears, a new entry for the user appears in the Users pane of the Security Center, and you can return to the previous step to add the next user.

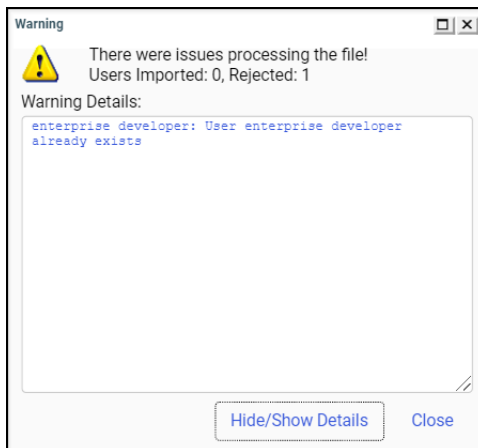
If you do not enter a description, the description defaults to the name. If you do not select a group and status for the user, the user will be created in the EVERYONE group and assigned the Active status, by default.

If you are creating a user that will be authenticated externally using AD or LDAP, and you want to synchronize user information with the authentication provider, leave the email and description fields blank.

### Importing Users

The Import User command automatically creates new user accounts by importing user information from a comma-separated values (.csv) text file and transferring those records to the user accounts database in the repository. This operation streamlines the creation of multiple user accounts by eliminating the necessity to open the New User dialog box, type, and save the details for each new user account, individually.

The import does not overwrite records of existing users, nor can you use it to delete existing user records. If a record in the user import file matches an existing user account, the import generates a message identifying the record that could not be imported, as shown in the following image.



### Understanding User Import File Layout and Format Requirements

You can create a new user import file by typing user information into any text editor and saving it as a comma-separated values (.csv) file. If you are exporting user information from an external source, you can create a user import file by reorganizing and reformatting the exported information, as necessary, and then saving the exported user information in a .csv file. Regardless of the method you use, you must ensure that all user import files you create conform to the format and layout requirements described in this topic and that the information within those user records conforms to the requirements described in [Understanding User Record Field Format Requirements](#) on page 449.

The user import file must not contain a header or column heading line. The first line in the file must contain the first user record. From that point on, each line within the user import file contains the record for a single new user. Multiple user records must not be placed on the same line. Because the import will end when it encounters the first blank line, do not include any blank lines between user records.

User import files that contain only those NLS characters used in the U.S. English or Western Europe code page 137 require no special encoding. However, user import files containing NLS characters from other code pages require UTF-8 encoding, without a byte order mark (BOM). To encode a user import file for UTF-8, open it in a third-party editor, change the appropriate setting to specify that the file uses UTF-8 encoding, and save it with that value.

Each user record contains the following fields: user name, password, description, email address, user status, and groups, as shown in the following image.

```
testbas,password,Getting Started Basic User,testbas@domain.com,ACTIVE,Getting_Started/BasicUsers
testadv,password,Getting Started Advanced User,testadv@domain.com,ACTIVE,Getting_Started/AdvancedUsers
testdev,password,Getting Started Developer,testdev@domain.com,ACTIVE,Getting_Started/Developers
testgrp,password,Getting Started Group Admin,testgrp@domain.com,ACTIVE,Getting_Started/GroupAdmins
testdevgrp,password,Getting Started Dev-Grp Admin,testdevgrp@domain.com,ACTIVE,Getting_Started/Developers;Getting_Started/GroupAdmins
testbas2,password,Getting Started Basic User 2,testbas@domain.com,INACTIVE,Getting_Started/BasicUsers
testbas3,password,Getting Started Basic User 3,testbas@domain.com,MUSTCHANGE,Getting_Started/BasicUsers
```

Within a user record, each field is separated by a comma. If the value assigned to a field includes a comma, the value in that field must be enclosed within quotation marks ("). For example the following new user record contains a comma in the third field, the description field, and is enclosed in quotation marks ("):

```
testadv,password,"Getting Started, Advanced
User",testadv@workspace.com,ACTIVE,Getting_Started/AdvancedUsers
```

If a field in a user record contains no information, the record must still define a placeholder for the blank field by leaving two commas with no characters between them in the appropriate place in the record. For example, the following new user record omits the password typically found in the second field of a user entry:

```
testbas,,Getting Started Basic User,testbas@workspace.com,ACTIVE,Getting_Started/BasicUsers
```

## Understanding User Record Field Format Requirements

When creating a user record, ensure that the values you assign to individual fields conform to the following requirements:

- ❑ **User Name.** Names assigned to imported users are subject to the same restrictions on valid characters as those entered directly in the new user dialog box. For a detailed description of user names and the range of characters that you can include in them, see [Understanding User Name Requirements](#) on page 446.

**Note:** When importing users to a tenant workspace that requires the use of a namespace, there is no need to type the namespace in this field if you have assigned the PREFIX or SUFFIX value to the Add Namespace When Creating Users by Group Administrators (IBI\_USER\_NAMESPACE) setting. The User Import process assigns the relevant namespace automatically when creating the new user record, and uses the format assigned to that setting. As a reminder, this feature is relevant only to users imported to a tenant workspace by a Group Administrator. For more information, see the definition for the Add Namespace When Creating Users by Group Administrators (IBI\_USER\_NAMESPACE) setting, as described in [Using Advanced Settings](#) on page 149.

- ☐ **Password.** You can assign a generic one-time password, such as *password*, to the password field, or you can assign one of the hashed passwords from the UOA\_USERS table.
- ☐ **Description.** Leave this field blank if you have activated the Synchronize User Information setting, which is located on the External page of the Security tab of the Administration Console. Otherwise, type the full name of the user or a brief description in this field. The activation of the Synchronize User Information setting allows for automatic updates to the value in this field from an external authentication or authorization provider.
- ☐ **Email Address.** Leave this field blank if you have activated the Synchronize User Information setting, which is located on the External page of the Security tab of the Administration Console. Otherwise, type the email address for the new user. The activation of the Synchronize User Information setting allows for automatic updates to the value in this field from an external authentication or authorization provider.
- ☐ **User Status.** Type ACTIVE, INACTIVE, or MUSTCHANGE in this field to identify the initial status of the user when the new user account is created. Each of these values must be typed in uppercase characters. If you type ACTIVE, the user represented by the account can sign in and begin working as soon as the account is created. If you type INACTIVE, the user represented by the account can sign in and work only after an administrator has changed the status of that user account to Active. If you type MUSTCHANGE, the user represented by the account is prompted to change his or her one-time password the first time he or she signs in.
- ☐ **Groups.** Type the name of the group or groups to which the user is assigned. If you do not include a value in the group name field, the user will be assigned to the EVERYONE group automatically. If you do include a group name, make sure that it matches the spelling and capitalization of its corresponding existing group name exactly.

The format for a group name is the workspace name, followed by a slash mark (/), and the group name. For example, the following new user record adds a user to the AdvancedUsers group of the Getting\_Started workspace, as shown in the last field in the record.

*testadv,password,Getting Started Advanced  
User,testadv@workspace.com,ACTIVE,Getting\_Started/AdvancedUsers*

You can include more than one group name in this field. If you choose to do so, separate each group name with a semi-colon. For example, the following new user record adds a user to the Developers group *and* to the GroupAdmin group within the Getting\_Started workspace, as shown in the last field in the record.


*testdevgrp,password,Getting Started Dev-Grp  
Admin,testdevgrp@workspace.com,ACTIVE,Getting\_Started/Developers;Getting\_Started/  
GroupAdmins*

To prevent a user record from failing to load, any group that you identify in it must already be defined within WebFOCUS. You cannot use the import user operation to load new groups as well as users simultaneously.

**Note:** If you are importing users to a tenant workspace as a Group Administrator, you will be unable to assign new users to groups within that workspace. To avoid generating errors, include the name of the tenant workspace only in this field and exclude the slash mark and group name.

### **Procedure:** How to Import Users

Before you begin, ensure that all groups that are identified in the user import file already appear in the Groups pane of the Security Center, and create any groups or workspaces that do not appear.


1. In the Security Center, on the Users & Groups tab, click *Import Users* .
2. In the Import Users dialog box, click *Browse*.
3. In the Choose File to Upload dialog box, navigate to the .csv file that contains the users to import and double-click the entry, or click it, and then click *Open*.
4. In the Import Users dialog box, ensure that the name of the file that contains user records for import appears in the File to Import field, and if so, click *Import*.


The import operation creates new user accounts for the users specified in the file records, and assigns the new users to the groups specified in each record.

- a. If you receive a message stating that there were issues processing the file, click *Hide/Show details*, review the issues listed in Warning Details dialog box, and update the import user file text or layout to address them.
- b. When your updates are complete, save the revised user import file, close the Warning Details dialog box, and return to step 2 to run the import again.

5. When the import is complete, click *Close* in the Import Users dialog box.
6. Review the Users pane and the Users in Group pane to ensure that the full set of new users was imported, and that they were appropriately assigned to all groups.

### **Procedure:** How to Edit User Details


1. In the Security Center, on the Users & Groups tab, double-click a user, right-click the user and select *Edit*, or select the user and click the *Edit User* button . The Edit User dialog box opens, as shown in the following image.



2. If desired, type new information in the *User Name*, *Description*, or *EMail Address* field.
3. To change the status of a user, select *Active*, *Inactive*, or *Must Change Password* from the Status drop-down list.

**Note:** If you select *Must Change Password*, users will be prompted to change their password when they attempt to sign in.

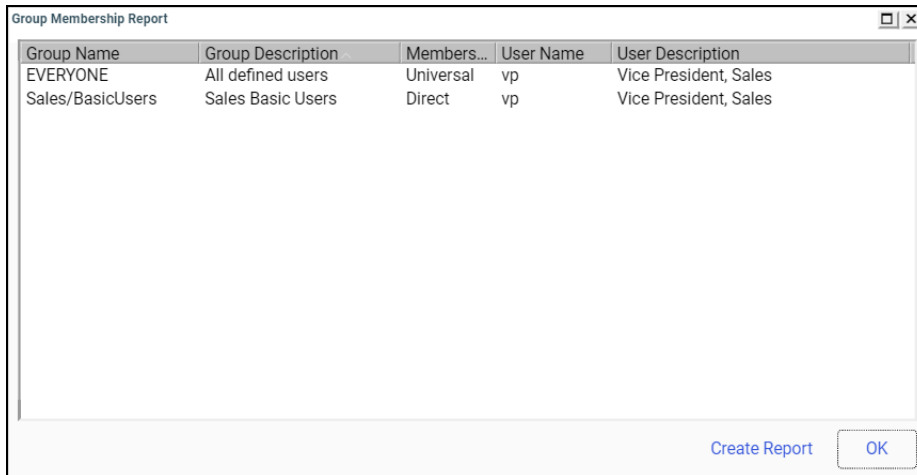
### **Procedure:** How to Delete a User

In the Security Center, on the Users & Groups tab, right-click a user and select *Delete*, or select the user and click the *Delete User* button .



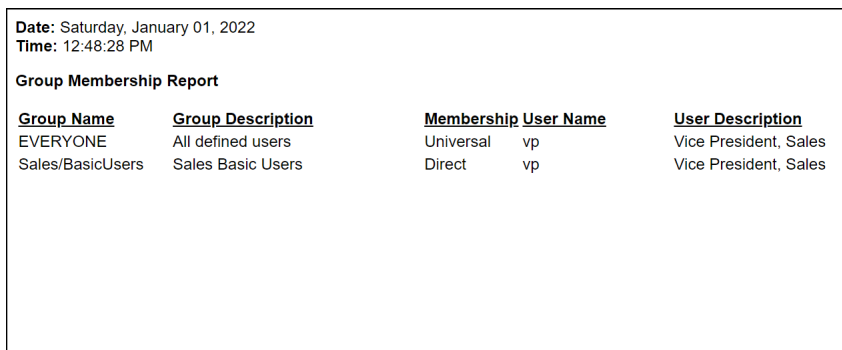
## Understanding the Group Membership Report

The Group Membership report lists all groups to which an individual user or selected group of users is currently assigned. The list entry for each group assignment identifies a Group Name, Group Description, User Name, and User Description, as shown in the following image.



By default, the report lists entries in ascending order by Group Name. You can reorganize this default display by clicking column headings to sort the report entries in ascending or descending order based on the values in that column.

From this dialog box, you can also create an HTML version of the report, as shown in the following image.



Using commands in your browser, you can save this version of the report or send it by email to an external reviewer.

The Date and Time that appear on the HTML version of the Group Membership report use the default, locale-sensitive time format (24 hours or 12 hours AM/PM) assigned to the computer on which WebFOCUS is installed. Therefore, if you select a different language when you sign in, dates and times continue to appear in the format used by the default locale of your machine instead of the format required by the language you selected.

For example, if your installation is hosted on a machine that runs on the Windows operating system, uses English as the default language, and uses a locale-sensitive time format of 12 hours AM/PM instead of 24 hours, all times are displayed in the 12 hour AM/PM format. Even if you configure WebFOCUS to use the UNICODE code page and include the Japanese locale in the Dynamic Language Switch settings, times on this report and throughout the user interface continue to use the 12 hour AM/PM format. You cannot change the time display to a 24-hour time format unless you also add Japanese to the Windows Language configuration and change to a 24-hour time format within the Windows Date and Time settings on the machine that runs WebFOCUS.

### ***Procedure:*** How to Create a Group Membership Report

The Group Membership report is available only to Administrators and users to whom the Security Center is also available.

1. In the Security Center, do one of the following:

- ☐ To base the report on an individual user, in the Users pane, right-click the entry of your selected user.
- ☐ To base the report on a group of adjacent users, in the Users pane, click the first user entry, hold down the Shift key, click on the final user entry, and then right-click your selection.
- ☐ To base the report on a group of non-adjacent users, in the Users pane, hold down the Ctrl key, click on all of the individual entries you want to include in the report, and then right-click any selected entry.

2. When your selections are complete, in the shortcut menu, point to *Groups*, and then click *Group membership report*.

The Group Membership Report dialog box opens, displaying all group assignments for your selected users.

3. To rearrange the report entries, click any column heading to list report entries in ascending or descending order based on the values in that column.
4. To produce an HTML version of the report, click *Create Report*.

Use the commands in your browser menu to print, save, or send the report.

5. To close the dialog box, click *OK*.

## Managing Groups

The Groups field in the Users & Groups tab of the Security Center lists all of the groups in the repository in hierarchical order. In the Groups field, subgroups are indented below their parent groups. The Users in Group field lists the members of a selected group. If no group is selected, the field is blank. The Search field in this tab allows you to search the name and description fields for groups. Simple wildcard searches are supported. A toolbar allows you to perform the following actions:

- ☐ Create, edit, or delete groups.
- ☐ View the members of a group.

## Understanding Groups

A group is a collection of users or subgroups that require similar capabilities or access to the same resources. Although rules may also be applied to individual user roles, typically, the activities and resources made available to users depend upon the rules that apply to the groups to which they belong. Therefore, group assignments are a pivotal component of security policy implementation.

All users are automatically assigned to the **EVERYONE** group, by default. This group is the set of all named users in the system. Administrators must then assign users to the appropriate groups within the workspaces that contain the content resources they will need to use and to the appropriate groups within My Workspace and the Getting Started workspace.

By default, a newly created workspace includes four groups, Basic Users, Advanced Users, Developers, and Group Administrators. Each of these groups contains a pre-defined range of privileges that support the activities and resource needs of a typical user in that role. Preconfigured infrastructure groups, including My Workspace and the Getting Started Workspace, vary from this basic configuration.

Administrators can also create their own groups. These groups can supplement the original four groups within an individual workspace or they can be a specialized group that is assigned to multiple workspaces.

Users can belong to more than one group, and each group can contain a different set of privileges. The ability to assign users to different groups allows administrators to provide varying levels of access to the same user.

### **Workspace Groups**

The following groups are assigned to new workspaces automatically. They represent the most common types of users, and the privileges assigned to them support the typical set of activities that members of such a workspace group would be expected to perform.

When created from the resource template, these groups are generated automatically for each new workspace, and four of them, Basic Users, Advanced Users, Developers, and Group Administrators, are made available to the new workspace, by default. A fifth group, the Authors group, is available only in My Workspace and the Getting Started workspace.

### **Basic Users**

Members of the Basic User group can view content within their workspaces. They can create folders within the My Content folder and save deferred reports to them. They can also copy autolink parameters from a previously-created report and save them in their folders. They cannot share, publish, copy, or paste any folder or content item.

### **Advanced Users**

Members of the Advanced User group can view content within their workspaces. They can create folders within the My Content folder and save deferred reports to them. They can also copy autolink parameters from a previously-created report and save them in their folders, and they can create and share their own content items and folders.

### **Authors**

This group is available only in the pre-configured workspaces entitled My Workspace and Getting Started. Members of the Authors group can view content, create folders, and save deferred reports to their folders. They can also copy autolink parameters from a previously created report and save them in their folders, and they can create and share folders and content items. In addition to these privileges, these self-service analytical users can connect to data, open data files, and create portals when working in their personal My Workspace view or in the Getting Started view.

## Developers

Members of the Developers group can view content within their workspace. They can create folders within the My Content folder and save deferred reports to them. They can also copy autolink parameters from a previously-created report and save them in their folders, and they can create and share their own content items and folders. They can upload and connect to data, edit metadata, and create and organize workspace content. They can manage content made visible to other users. They can also copy and paste folders and content from their workspace to another workspace, but they must be sure that the workspace they target for this operation maintains connections to the same metadata as that used to create the content they are copying.

## Group Administrators

Members of the Group Administrators group can determine the role each user can have within a workspace by adding users to or removing users from one of the five user type groups and can change the General Access setting assigned to a workspace. They do not have access to reporting or development capabilities.

These five user types cover the basic access levels that the majority of users will require when working with workspaces, freeing administrators to focus on the assignment of users to these five groups instead of requiring them to configure unique access level profiles for each user.

## Infrastructure Groups

The following groups are created automatically during the product installation. They provide a role for users when working outside of workspaces created to support content development.

## My\_Workspace Group

The My\_Workspace group contains users who are assigned to the specialized workspace entitled My Workspace.

My Workspace is created from the standard resource template and uses the same security rules assigned to all templates. However, instead of the four groups that are typically assigned to workspaces, it contains only the Basic Users group and the Authors group. The privileges defined for these two groups apply when users are working within the My Content folder of My Workspace.

As with any other workspace, administrators must actively manage the assignment of users to the two groups within My Workspace. Privileges granted to a user in My Workspace are entirely independent of privileges granted to a user in any other workspace.

Some product installations may use a different workspace as the default workspace for content created directly from the Hub, the WebFOCUS Home Page, or outside of an existing workspace. They do so by defining a path to that alternative workspace in the Default Workspace Repository Path (IBI\_DEFAULT\_WORKSPACE\_PATH) setting on the BI Portals settings page in the Administration Console.

Note that this configuration does not eliminate My Workspace or the groups assigned to it. Even when an alternative workspace is identified in the Default Workspace Repository Path, users assigned to sub-groups within the My Workspace group can still open My Workspace from the content view of the WebFOCUS Home Page and run or create new content as made possible by their My Workspace group assignment.

### **Administrators Group**

Members in the Administrators group have full access to all workspaces and product features. Users in this group are assigned to the SystemFullControl role, by default. The default administrator, identified with the admin user ID, is assigned to this group. You can supplement this default administrator, whose password is provided during installation and therefore potentially known by multiple individuals, with other users who have their own unique password.

### **Anonymous Group**

Members in the Anonymous group have access, within the limitations imposed by the rules assigned to this group, to any resource made available to the EVERYONE group. Members in the Anonymous group are assigned to the BIDRunTimeAccess role, by default, which provides limited access to content resources. They are also assigned to the AnonymousRestrictions role, which prevents them from developing or copying resources. They can review and run resources only in My Workspace and in any other workspace made available to public users.

The public user is assigned to this group by default. The WebFOCUS Client automatically assigns this user ID to all unauthenticated requests to access resources within the WFC/Repository/Public folder and in the workspace folders to which the administrator has granted list and run access. A separate session is created for each anonymous user.

The user ID assigned to this default anonymous user is defined in the Anonymous User ID (IBI\_ANONYMOUS\_USER) setting on the Advanced Security page of the Administration Console Security tab. The name public is assigned to this setting, by default. Hence, in most installations, the default anonymous user is identified as the public user.

## EVERYONE Group

Members in the EVERYONE group have Basic User access to all workspaces. They can view and run resources in workspaces but they cannot create content nor can they modify existing content in any other workspace but their own. Users are, by default, members of the EVERYONE group in addition to their assignment to other groups.

## Managers Group


Members in the Managers group have access to all workspaces. They are assigned to the WebFOCUSManager role throughout the application, which provides a broad range of privileges that enables them to manage WebFOCUS operations.

## SelfServiceDevelopers Group

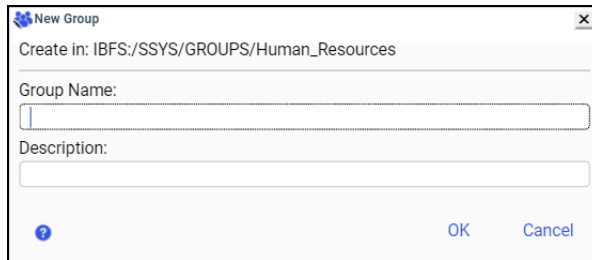
Members in the Self Service Developers group have access to all system features. This specialized group of users applies only to customers who use WebFOCUS with a self-service license. These users work with a version of WebFOCUS that replaces the default user interface with an independently designed and developed user interface.

This group includes the Wfdesktop user ID, which is the default ID to access the Desktop tools. Members of this group can perform self-service development work in the Data Servers, and Web Applications areas. Access to the Repository is restricted to the access given to the Everyone group.

### **Procedure:** How to Create a Group

1. In the Security Center, on the Users & Groups tab:
  - ☐ To create a group, click the *New Group* button , or right-click the Groups level of the hierarchy and select *New*.
  - ☐ To create a subgroup (nested group), select the group under which you would like to create a subgroup, then click the *New Group* button. Alternatively, right-click the parent group and select *New*.

The New Group dialog box appears, as shown in the following image.




If external groups are enabled, the dialog box will also allow you to type or browse and select from external groups.

The Create in: location is determined by where you placed your cursor before you clicked New Group.

2. Type the group name and an optional description, and then click *OK*.

The group name may consist of alphanumeric characters and underscores, but blank spaces, and the characters \* / | ; " , ? are prohibited. A group name may contain up to 255 characters. The description may consist of any characters allowed in your system. If you leave the description blank, WebFOCUS will automatically assign the group name as the description. You can edit the name or the description at any time.


### **Procedure:** How to Edit a Group

1. In the Security Center, on the Users & Groups tab, right-click a group and select *Edit*, or select the group and click the *Edit Group* button .

The Edit Group dialog box opens.

2. Edit the group name or the description as desired, then click *OK*.


### **Procedure:** How to Delete a Group

1. In the Security Center, on the Users & Groups tab, right-click a group and select *Delete*, or select the group and click the *Delete Group* button .
2. When you receive a message asking if you want to delete all selected items, click *Yes*.

### **Procedure:** How to Add a User to a Group

1. Open the Security Center.



2. On the Users & Groups tab, perform one of the following operations:
  - a. Drag the user you wish to add to the group from the Users field into the Groups field, and drop it on the Name of a group or subgroup.
  - b. Click a group or subgroup in the Groups field, and drag the user you wish to add to the group from the Users field into the Users in Group field.
  - c. Click a group or subgroup in the Groups field, click the user you wish to add to the group in the Users field, and then click the *Add selected users to group* button .

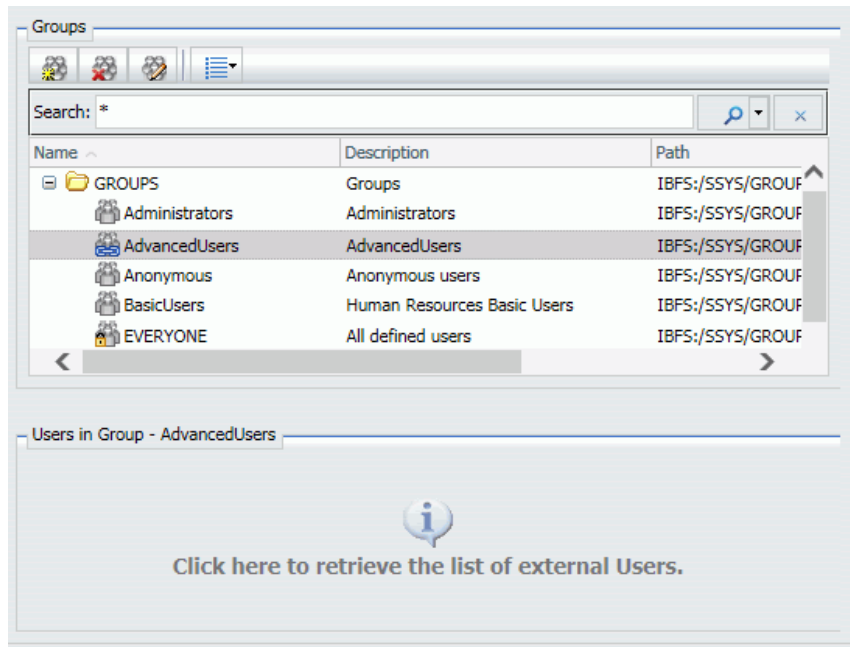
When your selected operation is complete, the user you added appears in the Users in Group field.

**Notes:**

- ☐ When you drag a user over a group in the Groups field, the group expands automatically, enabling you to drop the user on the name of a subgroup within that group.
- ☐ If external group mapping is not activated, the members of the selected group appear in the Users in Group field when you click a group or subgroup.
- ☐ If the WebFOCUS group is mapped to an external group, you cannot assign users directly to that group.


**Procedure: How to View External Users in a Group**

1. In the Security Center, on the Users & Groups tab, under Groups, select a mapped group, as shown in the following image.



2. Click the Users in Group field.  
The external users are listed.

### ***Procedure:*** How to Remove a User From a Group

1. In the Security Center, on the Users & Groups tab, under Groups, select a group.
2. Select a user and click the *Remove selected users from group* button , or drag the user into the Users field.  
You can also remove a user from a group by right-clicking on the user and clicking *Remove*.

## Managing Roles

The Roles tab lists the name of each role, the subsystems to which it applies, and a description of what it does, as shown in the following image.

Name	Used With	Description
ROLES		Roles
AllowAutocreateMyCo	WFC	Enable checkbox/property to allow creation of My Content folders
AnonymousRestrictior *		Used to prevent specific privileges from being assigned to Anonymous users
ApplyAccessLists	WFC	Apply Access if on access list
BIDRunTimeAccess	Session	BID runtime access
BIDViewBuilder	GROUPS	BID ViewBuilder access
BIPCreatePortal	BIP,WFC	BIP create portal
BIPFullControl	BIP,WFC	BIP full control
BIPViewAndCustomiz	BIP,WFC	BIP view, save positions and add content
BIPViewOnly	BIP,WFC	BIP view only
CreatePrivateFolder	WFC	Create private folders
Distribution Directory / *		User maintains access to distribution directory
Distribution to the File *		User can distribute output to the File System
DomainAdvancedUser	Session,WFC,BIP,EDA	Basic users who can also create personal analytic content and use some sct
DomainAuthor	Session,WFC,BIP,EDA	Self service analytical users who can upload, connect to, and visualize data
DomainBasicUser	Session,WFC,BIP	Users can run procedures, access library content, and personalize portal view
DomainDeveloper	Session,WFC,BIP,EDA	Advanced users who can also develop workspace reporting applications and
DomainDeveloperChar	GROUPS	Limits who developers can change ownership to
DomainDeveloperRest	WFC,BIP	Limits what developers can do on the workspace folder itself
DomainGroupAdmin	Session,WFC,BIP,GROUPS,ROLE	Enables group administrators to manage private content, group membership
DomainGroupAdminM	GROUPS	Enables group administrators to manage their users
DomainGroupAdminRe	WFC,BIP,GROUPS	Limits what group administrators can do on the workspace folder, workspac
DomainGroupAdminSc	GROUPS	Defines which users the group administrator can add to own managed group
DomainGroupAdminUk	ROLES	Defines which roles the group administrator can use in rules
Export	*	Export

\* Used with all Subsystems.

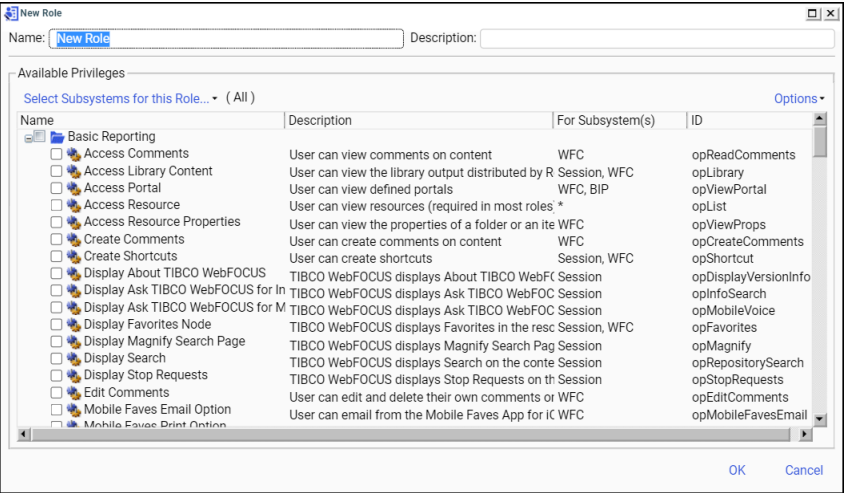
A role icon with a lock indicates that the role is read-only and cannot be edited or deleted. All pre-installed roles are read-only. Locked and pre-installed roles are not updated automatically when you choose to install a custom resource template. However, you may choose to revise them as part of your configuration of the custom resource template. For more information, see [Adding Customizations to the Custom Resource Template](#) on page 397.

Access to WebFOCUS Reporting Server applications is determined by the permissions assigned to any group that fits the access control template for that server instead of the pre-defined locked role. For more information, see [Understanding Access Control Templates](#) on page 401.

The Roles tab allows you to perform the following actions:

- ☐ Create, edit, delete, or clone a role.
- ☐ View or edit the access rules on a role.
- ☐ View or edit the effective policy on a role for a user or group.
- ☐ View the rules that use a selected role.

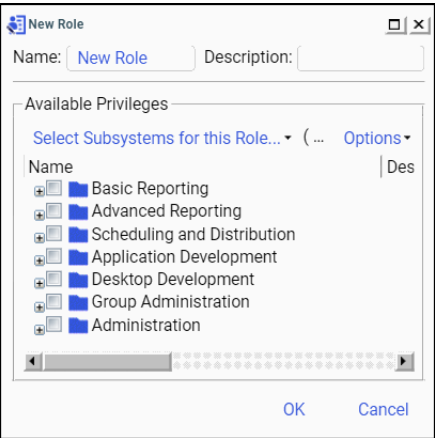
When you create or view a role, its privileges are displayed in a list that includes the privilege name, description, subsystems affected, and privilege ID, as shown in the following image.



If the description is too long to display, rest your mouse on it to display a tooltip with the full description. Resting your mouse on a privilege name brings up a tooltip that includes the privilege ID at the end, or you can scroll to the ID column. The privilege ID is a unique internal identifier and, except for Customer Support Services, is not generally used.

Privilege Categories

When you create a new role, you assign privileges to the role. To make the privileges easier to find, they are grouped into several categories, as shown in the following image and described in the following table.



Privilege Category	Description
Basic Reporting	Privileges that can be assigned to most users, including those with minimal training. All of the other sets of privileges are granted in addition to the basic reporting features.
Advanced Reporting	Privileges that can be assigned to users who need to create and share their own reports. They are generally granted as a supplement to the basic reporting privileges, not as a replacement for them.
Scheduling and Distribution	Privileges that can be assigned to users, developers, and administrators so they can create schedules that distribute reports with ReportCaster.
Application Development	Privileges that can be assigned to developers that enable them to create complete WebFOCUS applications using only web-based tools. To enable access to the full set of WebFOCUS application development capabilities, you should also assign the privileges in the Desktop Development category to your development team.
Desktop Development	Privileges that enable developers to use the Windows-based WebFOCUS desktop products. These privileges must be assigned along with those in the Application Development, Advanced Reporting, and Basic Reporting categories to enable the full set of development capabilities.
Group Administration	Privileges that can be assigned to department or tenant group administrators so that they can manage their users and the content created by their users.
Administration	System administrator privileges that are generally only assigned to WebFOCUS administrators.
Legacy	Privileges that enable legacy product behavior for customers migrating to WebFOCUS 8 from previous versions.

Within each category, privileges are listed in alphabetical order by their Name in English. The order of localized privilege names remains the same in all other languages, ensuring that privileges remain in a consistent order regardless of the language in which they are displayed. The use of a consistent location makes privileges easier to locate and identify.

You can select privileges individually by selecting the check box next to them or you can select an entire category of privileges by selecting the check box next to the folder for the category. You can also select a category and then remove some of the automatically selected privileges under that category.

The appearance of the check box next to the title entry for a category indicates the range of privileges selected within it. If none of the privileges within a category are selected, the check box is blank. If one or more of the individual privileges within a category are selected, the check box contains a block. If all of the privileges within the category are selected, the check box contains a check mark.

For more information about the privileges included in each category, see [Privileges](#) on page 635.

### **Reference: Subsystems**

Some privileges can apply to any subsystem, but most are limited to a particular kind of subsystem. For example, Access Portal only applies to the BIP (BI Portal) subsystem and Access Resource Properties only applies to the WFC (Content) subsystem and the EDA (WebFOCUS Reporting Servers) subsystem. Access Resource applies to every subsystem, which is indicated by an asterisk (\*) in the Subsystem(s) or Used With column. Session indicates that the privilege is cached for the duration of the user session rather than applying to a specific subsystem.

When you create a role, all possible privileges are displayed. You can filter the list of privileges displayed by selecting Clear All from the Select Subsystems for this Role list, and then clicking the subsystems you intend to use with the role. Since the list closes each time you select a subsystem, to add multiple subsystems, you will need to open the list again for each new selection.


#### **Note:**

- ☐ When you remove subsystem settings from the list of subsystems for a role, you receive a message warning you that it will remove any configured privileges that do not match the new subsystem settings. When you select Clear All from the list, there is no warning and all privileges are removed from the list. If you inadvertently made this selection, click *Cancel* to dismiss the Role dialog box without saving your changes.

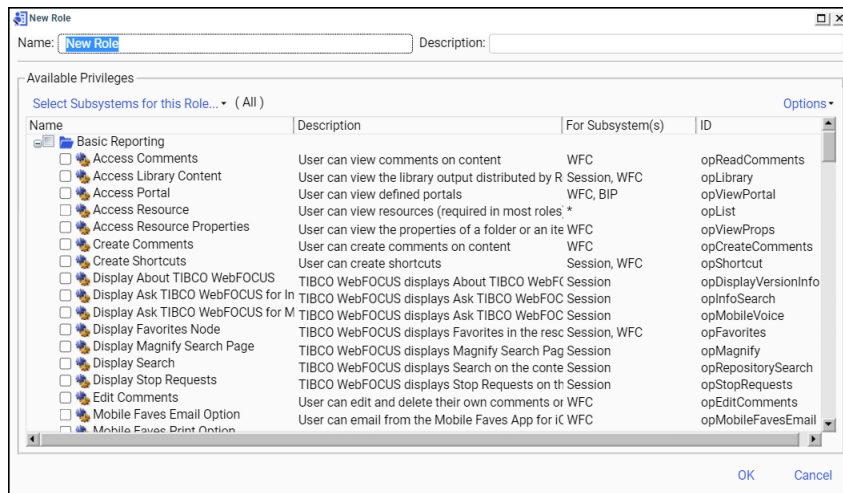
- ❑ When you add, delete, or replace a rule, WebFOCUS checks to ensure that you will still have access to the resources affected by the rule through the Access Resources (opList), and Manage Rules on Resources (opManageRulesOn) privileges for those resources. If the new rule would deny you access to these resources, the changes will not be saved and you will receive the ERROR\_RULE\_WOULD\_DROP\_CONTROL error.

For more information about subsystems and session privileges, see [Session Privileges](#) on page 348.

### Procedure: How to Create a Role

1. In the Security Center, click the *Roles* tab, and then click the *New Role* button .

The New Role dialog box appears, as shown in the following image.



2. Type a name in the *Name* field and a description in the *Description* field. If the *Description* field is blank, then the name is used.
3. If you want to omit any subsystems from this new role, open the *Select Subsystems for this Role* drop-down list and clear the check box for each subsystem you want to omit. The default selection is *All*.

**Note:** When you create rules for folder resources, this role will only be available for rules that apply to the selected subsystems and their children.

4. Perform one of the following steps to add privileges to the role:
  - a. Select the check box next to an individual privilege.
  - b. Select the check box next to a privilege category folder.

- c. Clear the check boxes next to any individual privilege or category that must not be included in the role.
5. Repeat the previous step as often as necessary.
6. Click *OK*.

The new role appears in the Roles tab list in alphabetical order by name.


### ***Procedure:*** How to Clone a Role

In the Security Center, click the *Roles* tab, right-click a role, and select *Clone*.


The new role appears below the original role with the extension *\_copy*.

**Note:** When you clone a role, the rules associated with the source role are dropped from the cloned role.

### ***Procedure:*** How to Edit a Role

1. In the Security Center, click the *Roles* tab, right-click a role, and then click *Edit*, or click a role, and then click *Edit Role*  to open the Edit Role dialog box.
2. To change the name or description, type the new value in the appropriate field.
3. To change the subsystem, select a new option from the Select Subsystems for this Role drop-down list.
4. Select the privilege category containing the privileges you wish to modify. If necessary, clear any individual privileges.
5. Repeat Step 5 for each privilege category you wish to update.
6. Click *OK*.

### ***Procedure:*** How to Delete a Role

1. In the Security Center, on the Roles tab, right-click a role and select *Delete*, or select the role and click the *Delete Role* button .
2. When you receive the Delete all selected items? confirmation message, click *Yes*.
3. Click *Yes* to proceed with the deletion.

**Note:** None of the default installed roles can be deleted.



## Migration Functionality and User Defined Roles (UDR)

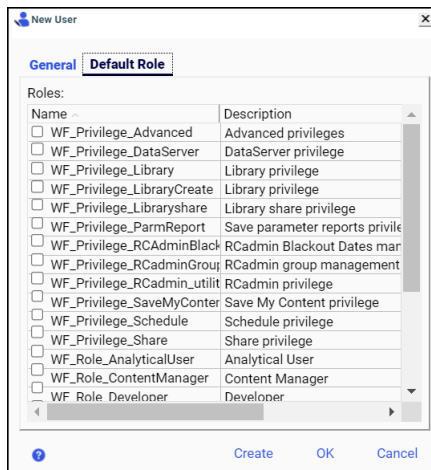
In WebFOCUS 7.x, users are assigned to a specific role and placed in a group or multiple groups. In WebFOCUS 8.x, user abilities are determined by rules based on groups, rather than user roles. The migration process maps WebFOCUS 7.x user roles to WebFOCUS User Default Roles (UDRs), which are implemented through rules, associated with the groups and workspaces, to which a user has access.

If you are using WebFOCUS 8 in a migrated environment, you can see UDR information by enabling the display of the User Default Role tab in the Security Center. For more information, see the *TIBCO WebFOCUS® Migration* technical content.

### **Procedure:** How to Display the User Default Role Tab in the Security Center

1. In the Administration Console, on the Configuration tab, click *Other* to display the Other settings page.
2. Select the User Default Roles (Used For Migration) (IBI\_ENABLE\_UDR) check box, and then click *Save*.
3. When you receive the Successfully Saved message, click *OK*.
4. Sign out of your current session.
5. Sign in again as an administrator, and navigate to the Security Center.
6. In the Security Center, click the *New User* button, or click an existing user, and then click *Edit User*.

The New User or Edit User dialog box opens, with the Default Role tab enabled, as shown in the following image.



## Managing Rules

Rules are always created by first selecting a resource from either the Resources tree or from within the Security Center. You can place rules on any resource, including:

- ☐ Folders
- ☐ Procedures
- ☐ Library output
- ☐ Portal pages
- ☐ WebFOCUS Reporting Servers
- ☐ Groups
- ☐ Users
- ☐ Roles

### ***Procedure:*** How to Create a Rule on a Content Resource

1. In the Resources tree or content area, right-click a node or content resource, point to *Security*, and then click *Rules*.
2. Select a subject.

- ☐ To select a group, click the group name.

- ☐ To select a user, first select the *Users* tab, then click the user name.

The list of available roles displays in the Rules for Group field, filtered to All Roles that can be used with this resource. Roles that are already being used in a rule with this resource and subject are bolded.

3. Select a role.

By default, all roles that can be used with the content resource will appear in the Rules for Group list. To limit the roles displayed, select one of the following filters from the Roles drop-down list:

- ☐ **Custom.** User-defined.
- ☐ **Common.** Often applied to resource type.
- ☐ **Roles.** Legacy Roles and Privileges.
- ☐ **Advanced.** Less often applied to resource type.

4. In the Access column, set the access for each role to Permitted, Denied, Over Permitted, or Clear Inheritance.

Not Set is the default and does not need to be selected unless another access type is inherited from a parent resource, which will be indicated in the Inherited Rule column.

5. In the Apply To column, set the scope of the rule to Folder and Children, Folder Only, or Children Only.

These settings can also indicate groups and subgroups, portals and portal pages, or any other objects that have a hierarchical relationship within IBFS.

6. Click *Apply* if you intend to continue and create additional rules for the selected subject on the selected resource, or click *OK* to save the current rule and exit the Security Rules dialog box.

### ***Procedure:* How to Create a Rule on a Group, User, or Role**

1. In the Security Center, on the Users & Groups tab, select a resource.

☐ To select a user, right-click the user name, point to *Security*, and then click *Rules*.

☐ To select a group, right-click the group name, point to *Security*, and then click *Rules*.

☐ To select a role, select the *Roles* tab, right-click the role name, point to *Security*, and then click *Rules*.

2. Select a subject.

☐ To select a group, simply click the group name.

☐ To select a user, first select the *Users* tab, then click the user name.

The list of available roles displays in the Rules for Group or the Rules for Users field, filtered to All Roles that can be used with this resource. Roles that are already being used in a rule with this resource and subject are bolded.

3. Select a role.

By default, all roles that can be used with the content resource will display. To limit the roles displayed, select one of the following filters from the Roles drop-down list:

☐ Custom - User-defined.

☐ Common - Often applied to resource type.

☐ Roles - Legacy Roles and Privileges.

☐ Advanced - Less often applied to resource type.

4. In the Access column, set the access for each role to Permitted, Denied, Over Permitted, or Clear Inheritance.

Not Set is the default and does not need to be selected unless another access type is inherited from a parent resource, which will be indicated in the Inherited Rule column.

5. In the Apply To column, set the scope of the rule to Folder and Children, Folder Only, or Children Only.

These settings can also indicate groups and subgroups, portals and portal pages, or any other objects that have a hierarchical relationship within IBFS. This selection becomes available only after you select a value for this rule in the access column.

6. Click *Apply* if you intend to continue and create additional rules for the selected subject on the selected resource, or click *OK* to save the current rule and exit the Security Center.

### ***Procedure:*** How to Remove a Rule From a Resource

1. In the Resources tree or content area, right-click a node or content resource, point to *Security*, and then click *Rules*.
2. Select the group or user that is the subject of the rule.
3. In the Access column of the Rules for User or Group list, set access to Not Set for each undesired role.
4. Click *Apply* if you want to make more changes, or click *OK* to save your changes and exit the Security Center.

### ***Procedure:*** How to View Rules on a Resource

To discover who has access to a resource, right-click the resource, point to *Security*, and then click *Rules on this Resource*. Select *Include Inherited Rules* to include rules that are in effect through inheritance. Click a column header to sort by that field. To produce a rich text version of the information displayed in the dialog box, click *Create Report*.

### ***Procedure:*** How to View Rules for a Group or User

To discover which resources a group or user can access, right-click the group or user, point to *Security*, and then *Rules for this Group* or *Rules for this User*. Click a column header to sort by that field. To produce a rich text version of the information displayed in the dialog box, click *Create Report*.

**Reference: Understanding the Rules on This Resource Dialog Box**

The Rules on this Resource dialog box displays all rules assigned to a selected resource, including those it inherited from parent resources. From this dialog box, you can review the rules assigned to your selected resource and produce a report based on this display for later review.

All resources maintain a set of rules that determine the ways in which different groups and users may interact with them. Each entry in the Rules on this Resource dialog box lists a rule assigned to a resource. The components of that rule link individual users or groups to a pre-configured role. The role assigned to a rule grants the users and groups linked to it the privilege to use a resource in a way that corresponds to their needs and responsibilities. The assignment of multiple rules to a resource ensures that the availability of that resource corresponds to the varying needs and responsibilities of a wide range of users.

Each rule contains the following components:

**Subject**

A group or user to which the rule applies. Groups and users are defined in the Security Center.

**Access**

The availability of a resource to a group of users. Values include Permitted, Denied, Over Permitted, or Clear Inheritance. This value also indicates whether or not a permission was inherited from a parent resource.

**Role**

A set of permissions used to take a specified action. Roles are defined in the Security Center.

**Apply To**

The range of resources in the hierarchy to which this rule applies. Values include Folder and Children, Folder Only, or Children Only. These settings can also indicate groups and subgroups, portals and portal pages, or any other objects that have a hierarchical relationship within IBFS.

**Set On**

The folder or sub folder within the Resources tree at which a specific rule was set. For example, if set to /WFC, the rule applies to all resources in the tree. If set to /WFC/Repository, the rule only applies to resources in the Repository node.

Additional features in this dialog box adjust the display of rules, and generate a report based on the display.

The Include Inherited Rules check box turns the display of inherited rules on and off. Select this check box to include roles inherited from folders or objects in the display.

The Create Report button produces a rich text version of the list of rules that you can save or print. The report created from this dialog box includes the date and time on which it was created along with the resource name. It serves as a record of the set of rules assigned to that resource at the specific time of the report.

### ***Procedure:* How to View Rules Which Use a Selected Role**

We recommend that you check where a role is used before deleting it.

1. In the Security Center, click the *Roles* tab.
2. Right-click a role, point to *Security*, and then click *Rules using this Role*.
3. To produce a rich text version of the information displayed in the dialog box, click *Create Report*.

## Managing Private Resources

Sometimes it is necessary for a manager to view or modify the private resources owned by another user. For example, when employees leave the company and their status is set to inactive, their private resources may need to be deleted or transferred to another user. It can also be useful for managers to have access to the private resources of the groups they manage in order to share resources or troubleshoot procedures. The Manage Private Resources privilege (opManagePrivateResources) grants a user or group the ability to manage the private content owned by a specified user or group. Typically, this privilege is *Permitted* for administrators on a group associated with a workspace and for group administrators on the groups they manage.

You can perform most actions on non-output resources owned by other users, such as FOCXECs, Reporting Objects, and schedules. For output resources, such as PDFs or Libraries, your abilities are limited to deleting the resources or changing their titles.

You can view and manage private resources by workspace or by user or group.

### ***Procedure:* How to Manage Private Resources by User or Group**

The Manage Private Resources feature allows you to identify and manage private resources owned by users or groups.

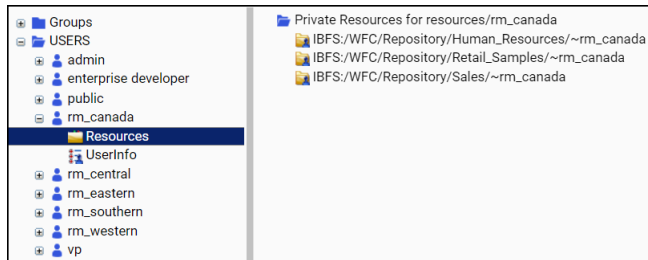
1. Sign in as an administrator.
2. On the Hub side navigation pane, select *Management Center*, and then .

Or

On the WebFOCUS Home Page, select *Settings*, and then select *Manage Private Resources* to open the Manage Private Resources dialog box.

3. Expand the individual user or group whose resources you would like to view or manage.

Selecting a group displays all resources owned by the group. Selecting a user displays resources and user information, as shown in the following image.



The user information contains full paths for user-specific location resources, such as private portals and home directories.

4. Right-click a resource that belongs to a member of your group and select an action from the shortcut menu.

You can perform most actions on non-output resources owned by other users, such as FOCXECs, Reporting Objects, and schedules. For output resources, such as PDFs or Libraries, your abilities are limited to deleting the resources or changing their titles.





## Securing a TIBCO WebFOCUS Environment

---

This topic describes WebFOCUS information assurance practices and security and encryption features. It recommends file system permissions for WebFOCUS components and certain precautions for protecting WebFOCUS variables.

### In this chapter:

- ☐ [Information Assurance Best Practices](#)
  - ☐ [Documentation](#)
  - ☐ [Open Web Application Security Project \(OWASP\)](#)
  - ☐ [ReportCaster Settings](#)
  - ☐ [TIBCO WebFOCUS Reporting Server Security](#)
  - ☐ [Differentiating TIBCO WebFOCUS Reporting Server Access Control and IBFS Security](#)
  - ☐ [Differentiating Data Security and IBFS Security](#)
  - ☐ [Protecting TIBCO WebFOCUS Variables](#)
  - ☐ [TIBCO WebFOCUS Encryption Features](#)
- 

### Information Assurance Best Practices

Information Assurance\* refers to measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. WebFOCUS contains a number of security capabilities that emphasize strategic risk management and defend against malicious hacker attacks. This level of security is critical for externally-facing web-based Business Intelligence applications.

WebFOCUS 8 has achieved a Level 2a validation using Open Web Application Security Project (OWASP) Application Security Verification Standards (ASVS), and a low vulnerability rating against the most important security vulnerabilities and threats in the industry, as defined by OWASP. For more information about Information Assurance and OWASP, go to [http://www.owasp.org/index.php/Main\\_Page](http://www.owasp.org/index.php/Main_Page).

\*Source: U.S. Government's National Information Assurance Glossary Superset of Security Integration.

## Documentation

The standards described in this chapter serve as a reference. For more information about the settings and controls discussed in this chapter, see the following manuals:

- ❑ *TIBCO WebFOCUS® Installation and Configuration Guide* for your platform
- ❑ *TIBCO WebFOCUS® ReportCaster Guide*
- ❑ *TIBCO WebFOCUS® Reporting Server Installation Guide*

## Open Web Application Security Project (OWASP)

The Open Web Application Security Project (OWASP) is an open community organization that is dedicated to improving the security of application software. All of the OWASP information, tools, documents, and forums are free to anyone interested in learning about web-based security and how to improve it within their environments.

The OWASP Top Ten Project provides a list of web vulnerabilities, as well as the remediation steps required to eliminate them.

OWASP also provides an Application Security Verification Standard (ASVS) document, which outlines a standard that can be implemented to test for web application security vulnerabilities.

For additional information on the Top Ten Project and the ASVS document, visit the OWASP website at [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page).

## ReportCaster Settings

The ReportCaster Distribution Server usually runs within a secured network environment, and encrypting these communication parameters is not usually necessary. If encryption from the Distribution Server to Managed Reporting is needed and encryption of the data to and from the WebFOCUS Reporting Server is needed, follow these steps:

### JSSE Caster

Set to YES within the ReportCaster configuration. This value enables the use of SSL from the ReportCaster Distribution Server communicating to the Managed Reporting Repository to schedule MR procedures.

### JSSE Servlet

Set to YES within the ReportCaster configuration. This value enables the use of SSL for the applet scheduling tools to retrieve MR procedures.

Set 3DES encrypt connection to WFRS, with the following additional parameter on the WebFOCUS Reporting Server JDBC URL:

```
jdbc:eda:\\hostname:port;server=;ENCRYPTION=1;
```

## TIBCO WebFOCUS Reporting Server Security

This section addresses TIBCO WebFOCUS Reporting Server security. For additional information, see the *TIBCO WebFOCUS® Reporting Server Administration* manual. Guidelines include:

- ☐ Install the WebFOCUS Reporting Server on a separate physical machine than the WebFOCUS Client.
- ☐ RESTRICT\_TO\_IP restricts incoming communications.  
Configure the WebFOCUS Reporting Server to accept incoming connections from a restricted list of hosts for the TCP/IP and HTTP connections. Use this and/or set up a firewall in between the WebFOCUS Client and the WebFOCUS Reporting Server.
- ☐ Use SSL to encrypt all data between the browser, the WebFOCUS Client, and the HTTP Listener for the WebFOCUS Reporting Server.
- ☐ Use AES encryption for TCP/IP communication from the WebFOCUS Client to the WebFOCUS Reporting Server.
- ☐ Disable operating system commands.

If applications do not require operating system commands, disable them using the Role Based Access controls on the WebFOCUS Reporting Server. On the Reporting Server browser interface, for a secure server, click the *Access Control* tab, and then click the *Basic User* role. In the General Privileges pane, select the *Disable Operating System Commands* check box.

☐ Disable the Direct Passthru option.

If applications do not require direct SQL Passthru, disable it using the Role Based Access controls on the WebFOCUS Reporting Server. On the Reporting Server browser interface, for a secure server, click the *Access Control* tab, and then click the *Basic User* role. In the General Privileges pane, select the *Disable Direct Passthru* check box.

☐ Encode HTML output data.

This setting will disable the rendering of HTML tags within a browser when these tags are stored within the actual data, or created using a DEFINE or COMPUTE command. On the Reporting Server browser interface, for a secure server, click the *Workspace* tab, right-click the *Workspace* folder and then click *Miscellaneous Settings*. In the *htmlencode* list, click *y*, and then click *Save*.

☐ Encrypt Master Files on the WebFOCUS Reporting Server.

☐ Encrypt WebFOCUS Reporting Server FOCXECs.

☐ SET DEFECCHO=NONE. This setting will disable echo output, so information regarding WebFOCUS code cannot be returned to the browser.

☐ Use DBA Security for those Master Files for which you want to restrict access.

## Differentiating TIBCO WebFOCUS Reporting Server Access Control and IBFS Security

It is recommended that you use IBFS rules to hide or expose WebFOCUS Reporting Server nodes when needed, but that you use WebFOCUS Reporting Server Roles and Access Control features to protect specific resources on the WebFOCUS Reporting Server. Rules applied to WebFOCUS Reporting Server resources below the node will not affect what is rendered in other parts of the user interface. They only apply to the Resources tree view. The WebFOCUS Reporting Server Access Control features provide much better security for controlling access to server engine settings, such as SQL pass-through or operating system commands, and to application folders which contain metadata and uploaded data.

## Differentiating Data Security and IBFS Security

IBFS security governs resources in the Repository and some external resources, such as WebFOCUS Reporting Server nodes. However, access to data rows in a database or field names in metadata is governed by Data Security (DBA) features. You can make use of these data security features by passing the authenticated user ID and user groups to the WebFOCUS Reporting Server.

For more information about exchanging information between the WebFOCUS Client and the WebFOCUS Reporting Server, see [Configuring the TIBCO WebFOCUS Reporting Server](#) on page 25.

## Protecting TIBCO WebFOCUS Variables

WebFOCUS scripts allow you to specify options for controlling variable processing. One of these options is the protect option, which prevents the variable from being set from the browser using the following syntax:

```
<SET> variable_name (protect)
```

WebFOCUS script commands are described in detail in [TIBCO WebFOCUS Script Commands](#) on page 710.

Variables you may want to protect include IBIF\_adhocfex and IBIF\_raw, both of which otherwise allow WebFOCUS to stream FOCUS commands to the WebFOCUS Reporting Server on the URL.

## TIBCO WebFOCUS Encryption Features

WebFOCUS uses encryption and encryption services in multiple ways, including:

- ☐ Encryption of the trusted connection between the WebFOCUS Client and the WebFOCUS Reporting Server.
- ☐ Encryption of service account information.
- ☐ Encryption of WebFOCUS script files.
- ☐ Encryption of WebFOCUS procedures and metadata.

An important element of security is confidentiality, which ensures privacy by encrypting sensitive information. When files are encrypted, they are secure from unauthorized examination. You use a key file to decrypt an encrypted file. Various forms of encryption include data, network session, and file-based encryption. You can optionally encrypt the WebFOCUS script files (.wfs), among the configuration files, by using the Client Settings and the Redirection Settings in the Administration Console. You can also encrypt the communication between the WebFOCUS Client and the WebFOCUS Reporting Server.

For more information about WebFOCUS Client settings, see *Encryption Settings*. For more information about Redirection settings, see [Understanding Redirection Settings](#) on page 129.

WebFOCUS 8 has its own encryption algorithm, but can also be configured to use the Advanced Encryption Standard (AES encryption), which is the industry standard. Legacy applications may require native WebFOCUS encryption.

Default TIBCO WebFOCUS Encryption and AES Encryption

WebFOCUS software supports the following forms of encryption:

- ☐ Default WebFOCUS encryption.
- ☐ AES (Advanced Encryption Standard) encryption.

You can enable alternate AES encryption providers in the Administration Console. The key length may be 128 bits, 192 bits, or 256 bits.

For information about configuring ReportCaster for AES encryption, see *Using the Zip Encryption Protection Default Plug-in* in the *TIBCO WebFOCUS® ReportCaster Guide*.

**Note:** Previous versions of WebFOCUS software supported custom security encryption providers based on custom algorithms. This feature has been deprecated in favor of AES encryption. If you require the use of a custom algorithm, consult Customer Support Services.

Reference: Key File Format

The encryption key information is stored in a plain text file and is represented by a sequence of characters in hexadecimal notation. Each eight bits of a key (or one byte) is represented by two hexadecimal characters. For example, a 64-bit (or 8-byte) key is represented by 16 hexadecimal characters. Each character is either a number (0-9) or a letter (A-F).

The following table specifies the number of hexadecimal characters required for encryption keys for the AES algorithm.

Key length in bits	Number of hexadecimal characters	Sample string	Algorithm
128	32	5468658A6C617A795468658A6C617A79	AES128
192	48	5468658A6C617A7920646F67206A756D7073206F7665723F	AES192

Key length in bits	Number of hexadecimal characters	Sample string	Algorithm
256	64	5468658A6C617A7920646F67206A756D 7073206F7665723F5468658A6C617A79	AES256

## Configuring Encryption in the TIBCO WebFOCUS Client

You can use the Administration Console to enable alternate encryption providers, configure external security tokens, encrypt WebFOCUS configuration files, and encrypt the trusted connection between the WebFOCUS Client and the WebFOCUS Reporting Server.

**Note:** If you are using an encryption key greater than 128 bits, the JVM used by your product installation must be using an unlimited strength Java Cryptography Extension (JCE) Jurisdiction Policy File. For more information, see the Oracle documentation at:

<http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html>

### **Procedure:** How to Enable an Alternate AES Encryption Provider

You can use the Administration Console to enable an alternate AES encryption provider and to specify an internal or external key.

1. Sign in as an administrator, and open the Administration Console.
2. Under the *Application Settings* folder, click *Encryption*.
3. Click the appropriate encryption provider in the Provider (IBI\_ENCRYPTION\_PROVIDER) list, as shown in the following table. If a key file is not listed, an internal key file will be used.

Encryption Algorithm	Option
AES 128 Encryption with Internal Key	ibi.webfoc.wfsecurity.encryption.wireaes. WFWireAES128
AES 128 Encryption with External Key	ibi.webfoc.wfsecurity.encryption.wireaes. WFWireAES128KeyFile
AES 192 Encryption with Internal Key	ibi.webfoc.wfsecurity.encryption.wireaes. WFWireAES192

Encryption Algorithm	Option
AES 192 Encryption with External Key	ibi.webfoc.wfsecurity.encryption.wireaes.WFWireAES192KeyFile
AES 256 Encryption with Internal Key	ibi.webfoc.wfsecurity.encryption.wireaes.WFWireAES256
AES 256 Encryption with External Key	ibi.webfoc.wfsecurity.encryption.wireaes.WFWireAES256KeyFile

If you are using an internal key, proceed to step 7. If you are using an external key, proceed to step 4. If you are using a security token, proceed to step 6.

4. Create the key file and save it as a plain text file.

For more information on hexadecimal keys, see [Key File Format](#) on page 482.

If you are using a security token to enable trusted communication between the WebFOCUS Client and other software, proceed to step 5. Otherwise, proceed to step 7.

5. If you are using a security token to enable trusted communication between the WebFOCUS Client and another application, enter the value of the token in the Token Key (IBI\_WF\_TOKEN\_KEY) setting and click Save.
6. Specify the value of the security token in the other application.

Consult the appropriate documentation for the other application you are using for more information on configuring the security token.

7. In the Administration Console, click the *Security* tab, and under the Security folder, click *Advanced*.
8. Enter one or more of the following server account credentials:

- ☐ IBI\_WFRS\_Service\_Pass
- ☐ IBI\_Anonymous\_WFRS\_Pass
- ☐ IBI\_Admin\_Pass
- ☐ IBI\_Magnify\_Repos\_DB\_Password

9. Restart the Application server.

The startup process automatically encrypts all new passwords in the configuration files.



**Procedure: How to Encrypt the Trusted Connection Between the WebFOCUS Client and the WebFOCUS Reporting Server**

You can use the Administration Console to encrypt the trusted connection between the WebFOCUS Client and the WebFOCUS Reporting Server. For more information about configuring the trusted connection, see [How to Configure the WebFOCUS Client to Make a Trusted Connection to the TIBCO WebFOCUS Reporting Server](#) on page 49.

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, expand the *Reporting Servers* folder and then expand the *Server Connections* folder.
3. Select the desired Reporting Server node.

The Client Configuration page appears.

4. Expand the *Advanced* node.
5. Click one of the following Encryption list options, and then click Save.

☐ **0.** Off.

☐ ***cipher(x)[-mode]***

where:

*cipher*

Is the encryption algorithm used, such as AES128 or AES256.

*x*

Optionally defines an RSA key length of 1024 bits. If unspecified, the default value used is 512 bits.

*mode*

Optionally, specifies the mode of operation, Electronic Code Book (ECB) or Cipher Block Chaining (CBC). If unspecified, the default value used is ECB.

6. Click Save.
7. When you receive the Saved Successfully message, click OK.
8. Specify the value of the security token in the other application.

Consult the appropriate documentation for the other application you are using for more information on configuring the security token.

9. Re-enter one or more of the following server account credentials in the configuration file:

- ☐ IBI\_WFRS\_Service\_Pass
- ☐ IBI\_Anonymous\_WFRS\_Pass
- ☐ IBI\_Admin\_Pass
- ☐ IBI\_Magnify\_Repos\_DB\_Password

10. Restart the Application server.

The startup process automatically encrypts all new passwords in the configuration files.

## TIBCO WebFOCUS Change Management

---

Change management is the process of moving application components between WebFOCUS environments of the same release level. Typically, application components move between WebFOCUS environments to ensure that applications have been fully tested, prior to their deployment to a production environment.

There are features and methodologies within WebFOCUS that are used to facilitate these important tasks.

### **In this chapter:**

- ☐ [Understanding the Change Management Process](#)
  - ☐ [Creating a Change Management Package](#)
- 

### **Understanding the Change Management Process**

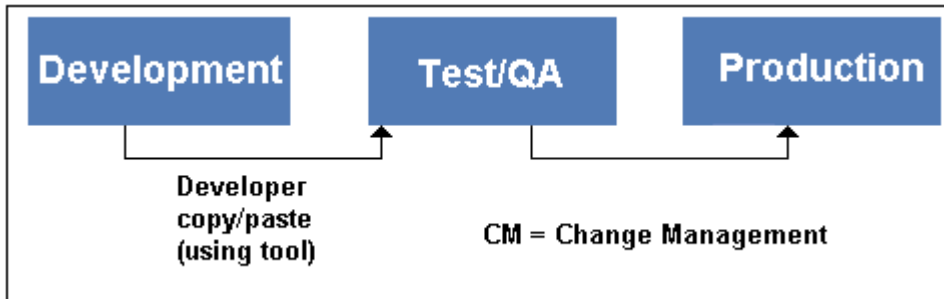
Developing an application is an iterative process. Developers revise application code and periodically move these components to the test environment for user feedback and acceptance. At some point within the application development lifecycle, when the application is stabilized, it is moved to production. After an application is released for general use, problems must be fixed, and the fixes must be tested and incorporated into the production environment. This is the essence of the change management process, which is also referred to as production control.

Organizations vary widely in how they approach change management. Some delegate much of the responsibility to developers, while others establish alternative processes to maintain a higher degree of control. Typically, developers utilize development tools to perform these duties, while change management professionals prefer batch-oriented methods to move application components between environments. Developers may be required to create change management packages in order to initiate changes after the application is moved to production. A combination of these approaches is often used in larger companies.

The examples that follow illustrate two different change management processes. These sections describe product features and methodologies that can be utilized by companies to meet their change management objectives.

**Example: Moving Application Files: A Simple Change Management Process**

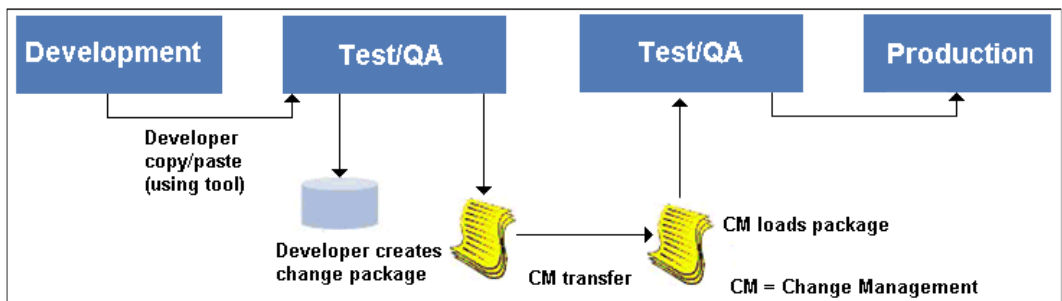
Developers move application files between the development and test environments using their development tool, as shown in the following image. When the application is finished, the application is copied from the test environment to the production environment, using operating system utilities. There may only be a single test environment.



**Example: Moving Application Files: A Comprehensive Change Management Process**

In this example, four environments are established to increase the level of control of moving application code to production. Developers use the Resources tree to move application files from the development environment to the test environment. Developers then use the Change Management Export facility, when they are ready to move their changes to the user acceptance test environment.

The Change Management Export facility allows the developer to select the resources to be moved and creates a change management package. An administrator can subsequently move the change management package into an acceptance test using the Change Management Import facility. Some organizations may choose to utilize an automated process to import the content, to achieve better integration with their business processes. As shown in the following image, when the application is ready for release, the production control personnel initiate a file system copy of the application to the production environment. Users begin using the application and the change management process shifts into an application maintenance support role. From this point forward, incremental updates to production are facilitated by administrators using the Change Management Import facility.



## Creating a Change Management Package

Many organizations do not grant developers write access to the user acceptance test and production environments. Access to these environments is strictly controlled and granted only to administrators, production control personnel, or automated change management processes.

Only developers know which changes are ready to be moved into the test environment. The Change Management Export facility presents developers with a graphical view of the resources they manage and allows them to build a change management package. This package is then loaded into another environment by production control personnel or automated processes.

A user must be authorized to create a change management package. The privilege to do so is Resource Export (opExport), a hybrid privilege, located in the Application Development privilege category. This privilege is assigned to members of the administrators group, by default.

The steps required to create a change management package are:

1. **Create a Scenario.** Using the Change Management Export facility, create a Change Management scenario by selecting the resources to export. A scenario is a description of all the resources included in a change management export package.

2. **Export a Scenario.** After creating a scenario, export it to the change management export directory as a change management package. The export process produces the package in two formats: a folder and a CM zip file. The folder contains the expanded contents of the change management package. The CM zip file contains the compressed contents of that package in a format that is ready to download and transfer to target environments.

The change management export directory is located within the file system of the machine that hosts WebFOCUS. The specific path varies by the type of installation used for your instance of WebFOCUS. Typically, this path is *drive:\ibi\context\cm\export*, where *context* represents the folders located between the ibi root directory and the cm directory.

3. **Download a Scenario.** For convenience, the CM zip file can be downloaded, using a web browser, from the export directory to a location outside of the change management directory. From this external location, the change management zip file is available for transfer to the import directory of the target WebFOCUS environment, where its content can be imported and accessed.

### Working With CM Zip Files

The zip file format compresses the resources that make up a change management package into a single file, delivering the advantages of speed and security to change management packages. They are especially useful when you must transfer change management packages from one physical location to another. Their compressed and consolidated format captures all files included in a change management package into a single file that can be emailed, copied, or moved from a source folder on one network component to a target folder on another.

Change management zip files, called CM zip files, are created, by default. To disable this feature, clear the Zip Change Management Package (IBI\_CM\_ZIP) check box, which is found on the Change Management page of the Configuration tab in the Administration Console. When this feature is disabled, change management packages use the uncompressed CM file format.

The default CM zip file name format is NAME\_DATE\_TIME\_USERID, which combines the name of the change management package, with the date and time on which it was created, and the ID of the user who created it.

For example, *retail\_samples\_20160504\_161133\_administrator.zip*.

To specify an alternative format for CM zip file names, select a template from the Name format of Zip export files (IBI\_CM\_ZIP\_FILE\_FORMAT) setting, which is found on the Change Management page of the Configuration tab in the Administration Console.

## Including Collaborative Portals in a Change Management Package

If your version of WebFOCUS supports collaborative portals, and the Collaborative Portal option is enabled, the change management process, from scenario creation to final import, readily accommodates collaborative portals. All of the topics that describe how to create, export, download, upload, and import change management packages support those that include collaborative portals as well as basic portals. However, there are a few issues to keep in mind when including collaborative portals.

When selecting a collaborative portal:

- ☐ To include all pages referenced by a collaborative portal in a change management scenario, select the folder that contains the pages referenced by that portal, and click the *Select With Sub-tree* command.
- ☐ Be sure to include any content referenced by a collaborative portal and its pages in a change management package.
- ☐ Because each portal within an environment must maintain a unique alias, be sure that none of the portals selected for import contains the same alias as any of the existing portals in the targeted environment. If one of the portals in an import package contains the same alias as an existing portal, the import process deletes the alias in the existing portal and retains it in the new portal. The process does not send a warning message advising you that the alias in the existing portal was deleted.
- ☐ You do not need to select the *Retain Handles* check box to include collaborative portals when creating change management packages. You will only need to do this if the content referenced by the collaborative portals has been migrated from WebFOCUS 7.7.x.

When importing a collaborative portal:

- ☐ Customizations made to collaborative portals remain intact in the targeted environment after the import.
- ☐ Customizations made to basic portals are lost and must be reconstructed in the targeted environment after the import.

Both private and published portals and focexec files can be included in the import package.

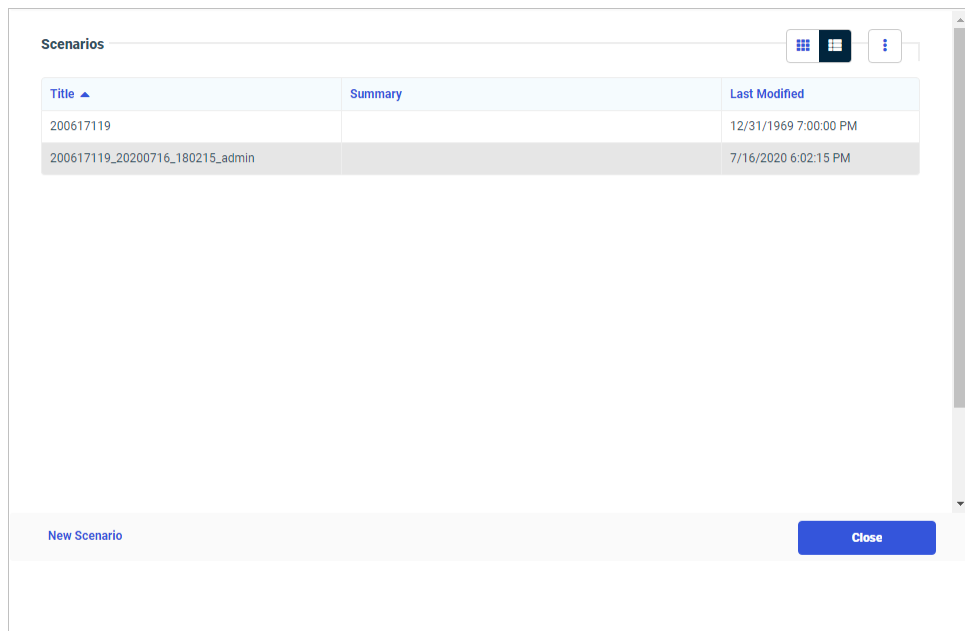
### **Procedure: How to Create a Scenario Using the Change Management Facility**

If your browser blocks pop-up windows, disable this feature before you begin using the change management facility, to ensure that you are able to see the dialog boxes that open during this procedure.

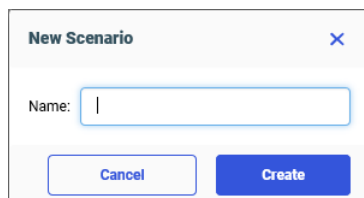
1. On the start page side navigation pane, select *Management Center* and *Export Packages*.

Or

On the WebFOCUS Home Page, in the banner, open the *Utilities* menu, and select *Change Management* and *Export* to open the Scenarios dialog box, as shown in the following image.

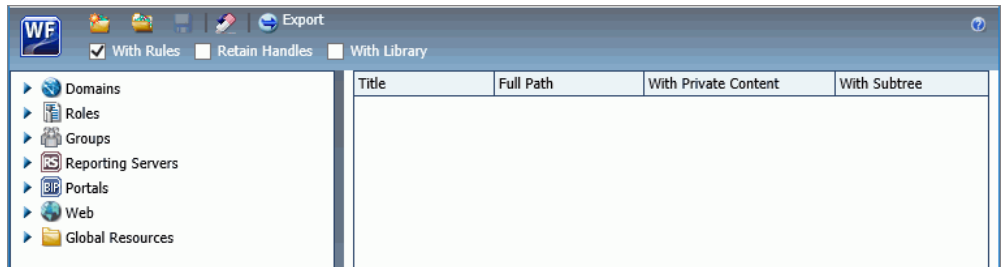


2. Select *New Scenario* to open the New Scenario dialog box, as shown in the following image.





3. In the New Scenario dialog box, enter a name for the scenario, and then select *Create* to open the Scenario dialog box, as shown in the following image.



The *With Rules* check box is selected, by default. Clear it only if this change management package should not include all rules associated with the resources you select.

**Note:** If you receive an alert in your browser stating that the pop-up window is blocked, reset your browser to allow all pop-up windows from this website, and try again.

4. To include content that has been migrated from WebFOCUS 7.7 to WebFOCUS 8 or ReportCaster schedules created in WebFOCUS 7.7 that reference procedures through an internal handle in the change management package, select the *Retain Handles* check box.
5. To include ReportCaster library content with any folder added to the scenario, select the *With Library* check box.

For more information about these three check boxes, see [Understanding Change Management Export Options](#) on page 499.

6. In the list of available resources, expand the node that contains the resource you want to include.
7. Right-click the resource you want to include, and perform the following steps:
  - a. Click *Select with Sub-Tree* to include a folder with all subfolders and their contents, or to include a group with all subgroups in your selection.

When selecting a collaborative portal that references external pages, you must also select the folder that contains the pages referenced by that portal, and then transfer them into the scenario by clicking the *Select with Sub-Tree* command.
  - b. Click *Select Folder Only* to include a specific folder, with no content. Typically, this is done to move rules on the folder.
  - c. Click *Select* to include a role, a portal, or an individual resource within a folder.
  - d. Click *Select Rules Only* to include rules from a Group or a WebFOCUS Reporting Server node.

- e. You can also select resources by dragging them from the Resources tree and dropping them in the right pane. When you do so, the *With Subtree* check box is selected, by default, and you must clear it if you wish to exclude subfolders and content from your selection.

When your selection is complete, an entry for it appears in the right pane, and a strikethrough line appears on the entry under the Resources tree.

- ☐ If you select a private resource, the *With Private Content* check box is automatically selected and can't be cleared.
  - ☐ If you select private content, it will only be imported if the owner of that private content already exists in the target environment.
  - ☐ If you select a published folder, you can include private content within it by selecting the *With Private Content* check box for that resource. This selection exports all of the private content in that folder and its subfolders, including those *My Content* folders that are assigned to individual users, even if you do not have the privileges necessary to view that private content.
  - ☐ If you select a subfolder without a parent folder, the Import process will recreate the parent folder in the target environment. A connection to the same metadata must exist within the target environment as well as the source environment.
  - ☐ When selecting a collaborative portal and pages that reference external content, be sure to include that content in the change management package.
  - ☐ If the rules on the source and target environments are different, users may have access to private content in the source environment, but be denied access in the target environment. This occurs if users have access to the published folder that contains the private content in the source environment, but do not have it in the target environment.
  - ☐ Even if the *With Library* check box is cleared, you can still include individual Report Libraries in a scenario by selecting them as described in this step.
  - ☐ The list of available roles does not include locked roles. Only unlocked roles are available for export in a change management scenario.
8. Repeat the previous step for any additional resources you want to include in the change management scenario.
  9. To clear your unsaved selections, in the New Scenario dialog box, on the toolbar, click *Reset Scenario*.
  10. When you have selected all resources, click *Save*.

An entry for the new scenario appears beneath the Export node.

If the new scenario does not appear, right-click the *Export* node, and then click *Refresh*.

To export the change management scenario using command line scripts, navigate to the following location and double-click one of the following commands:

`WebFOCUS82/utilities/cm/cm_export.bat`

`WebFOCUS82/utilities/cm/cm_export.sh`

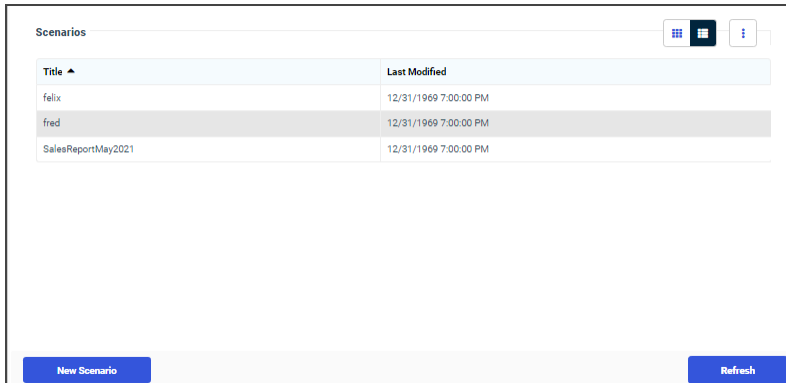
### **Procedure:** How to Transfer an Individual Collaborative Portal Page Using the Change Management Interface

If your version of WebFOCUS supports collaborative portals, and the Collaborative Portal option is enabled, you can use the Change Management Interface to transfer a page created for a collaborative portal in one environment to another environment where the same collaborative portal already exists. This procedure applies only to pages created for collaborative portals. It does not apply to pages created for basic portals.

1. On the start page side navigation pane, select *Management Center* and *Export Packages*.

Or

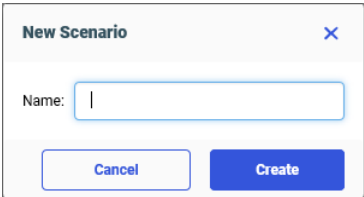
On the WebFOCUS Home Page, in the banner, open the *Utilities* menu, and select *Change Management* and *Export* to open the Scenarios dialog box, as shown in the following image.



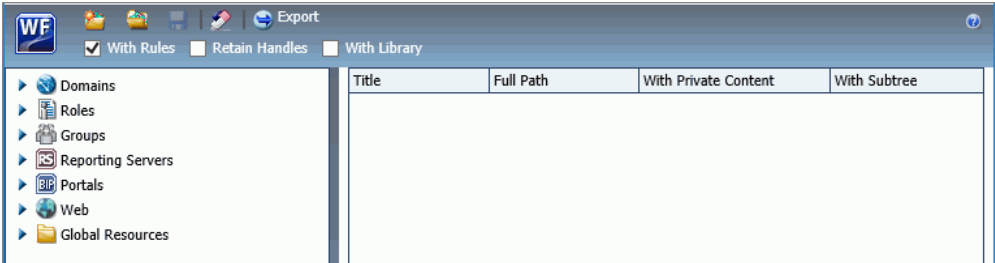
Title ▲	Last Modified
felix	12/31/1969 7:00:00 PM
fred	12/31/1969 7:00:00 PM
SalesReportMay2021	12/31/1969 7:00:00 PM

New Scenario Refresh

- 2. Select *New Scenario* to open the New Scenario dialog box, as shown in the following image.



- 3. In the New Scenario dialog box, enter a name for the scenario, and then select *Create* to open the Scenario dialog box, as shown in the following image.



The *With Rules* check box is selected, by default. Clear it only if this change management package should not include all rules associated with the resources you select.

**Note:** If you receive an alert in your browser stating that the pop-up window is blocked, reset your browser to allow all pop-up windows from this website, and try again.

- 4. Right-click the collaborative portal page that you want to transfer to the new environment, and then click *Select with Sub-Tree*.
- 5. Click *Save*.

An entry for the new scenario appears beneath the *Export* node.

If the new scenario does not appear, right-click the *Export* node, and then click *Refresh*.

- 6. Complete the transfer of the change management package as described in the remaining topics.

**Procedure:** How to Open a New Change Management Scenario from the Change Management Scenario Dialog Box

- 1. In the Change Management Scenario dialog box, on the toolbar, click *Create a new Scenario*.
- 2. If you receive a message that asks if you want to save the changes you made, click *Yes*.

3. Type the name of the new scenario, and click *OK*.

A new Change Management Scenario dialog box opens. The current Change Management Scenario dialog box also remains open.

4. Create the new scenario. For more information see, [How to Create a Scenario Using the Change Management Facility](#) on page 492.

**Procedure: How to Open an Existing Change Management Scenario from the Change Management Scenario Dialog Box**

1. In the Change Management Scenario dialog box, on the toolbar, click *Open existing Scenario*.
2. If you receive a message that asks if you want to save the changes you made, click *Yes*.
3. In the Open Scenario dialog box, navigate to the existing scenario you want to open and double-click it, or click it and then click *Open*.

Your selected Change Management Scenario dialog box opens and replaces the Change Management Scenario dialog box that was on display.

**Procedure: How to Export a Saved Change Management Scenario Using the Change Management Facility**

Before you can export a change management scenario, you must make sure that you have saved it. You can't export an unsaved change management scenario.

1. In the Change Management Scenario dialog box Quick Access Toolbar, click *Export*.
2. When the confirmation message opens, click *OK*.

The new scenario appears in the Resources tree under the Change Management, Export node.

If the new scenario does not appear, right-click the *Export* node, and then click *Refresh*.

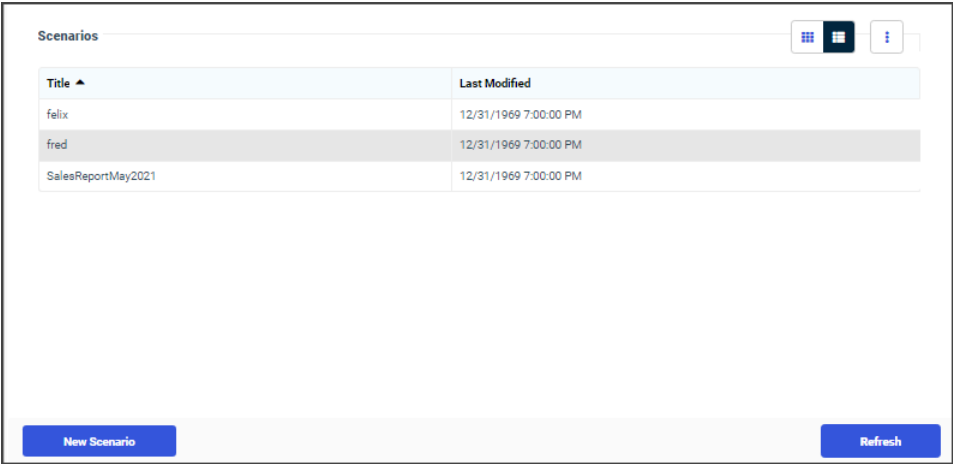
**Procedure: How to Download a Change Management Package Zip File**

The export process saves a CM zip file to the change management export directory, located at `drive:\ibi\context\cm\export`, where *context* represents the folders located between the ibi root directory and the cm directory. The download process takes that CM zip file, and downloads it to your local machine. You can then transfer the copy of that CM zip file to another WebFOCUS environment for use as a change management import package.

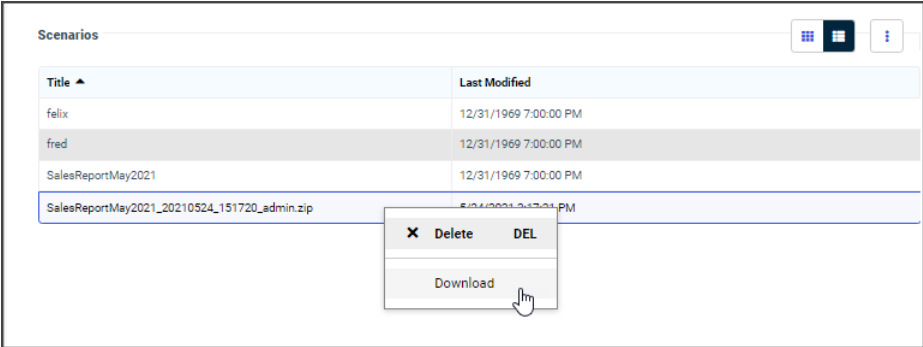
1. On the start page side navigation pane, select *Management Center* and *Export Packages*

Or

On the WebFOCUS Home Page, in the banner, open the *Utilities* menu, and select *Change Management* and *Export* to open the Scenarios dialog box, as shown in the following image.



- 2. Right-click the CM zip file you want to download and then click *Download*, as shown in the following image.



**Note:** When choosing between two list entries that include the same name, you can distinguish the full change management package from the zip file version by remembering that the name assigned to the zip file includes the name of the change management package from which it was taken, the date and time on which the package was created, and the ID of the user who created it. The name assigned to the full change management package does not contain any of these additional details.

- 3. Save the CM zip file to an external location as directed by your browser.
- 4. Close the Scenarios dialog box.

**Reference: Understanding Change Management Export Options**

The following export options are available from the Scenario Creation dialog box:

**With Rules.** Unselected, by default. When selected, this applies to the entire scenario and exports all rules associated with all of the selected resources. This will include all of the security components of those rules (groups, roles, and potentially users, if the subject of a rule). For example, if a single published folder of Sales is selected and there are rules on that folder for the subject of Sales/Dev Group, that particular folder of Sales will be exported, as well as all the constituent components of the rules on that folder and its subfolders.

**Retain Handles.** This option is necessary when you want to move content, such as content that has been migrated from WebFOCUS 7.7 to WebFOCUS 8, and ReportCaster schedules, using change management. When selected, this option specifies that the change management package uses the hrefs from WebFOCUS 7.7 as handles in WebFOCUS 8. It also ensures that ReportCaster schedules that were created in WebFOCUS 7.7, which reference procedures through the internal handle, continue to work. This allows the earlier code for -INCLUDEs and drill downs to continue to work with the WebFOCUS 7.7 syntax. ReportCaster schedules created in WebFOCUS 8 use the IBFS location of the Schedule object instead of the Handle and do not need the Retain Handles feature.

The default value for Retain Handles is specified by the Retain Handles (IBI\_CM\_Retain\_Handles) setting.

The following types of resources can be moved:

- ☐ Any folder or item from the /WFC/Repository or what is shown in the user interface as Content, including procedures (FOCEXECs), style sheets, images, HTML files, Schedules, Access Lists, and Distribution Lists.
- ☐ Any group or subgroup. Note that moving a group does NOT move user/group membership, and a subgroup can be moved without moving its parents.
- ☐ Any application or specific files from the WebFOCUS Reporting Server node on the tree. The File Types Included in Export Package (IBI\_CM\_EXPORT\_WFRS\_FILE\_EXTENSIONS) setting specifies which server content is visible and can therefore be exported. This value can be updated to add file extensions that are not included in the default list. The setting is intended only for application content, and not large data files, for performance reasons. If you need to move large data files, it is recommended that you do this by copying the files over from your source to target environment.
- ☐ Business Intelligence Portals.

**With Library.** When selected, the change management export scenario includes Report Library content in all folders you add to the export scenario. When cleared, the scenario does not include Report Library content in the folders you add to the export scenario. Even when this check box is cleared, you can still select individual Report Libraries for inclusion in a scenario. This check box is cleared, by default.

The Report Library is a secure facility that contains reports distributed to it by ReportCaster. For more information about the Report Library, see the *WebFOCUS ReportCaster* technical content.

### ***Procedure:* How to Run a Change Management Export Scenario Using the Command-Line Interface**

Now that you have created a scenario, that scenario can be exported. You can export a scenario through the Change Management User Interface or through an automated process, executed by running one of the `cm_export` scripts, which are located in the `cm` folder of the utilities directory, located at `drive:\ibi\context\utilities\cm`, where *context* represents the folders located between the ibi root directory and the `cm` directory.

As part of your preparations, ensure that the code page specified by the value in the `ENCODING` parameter in the `cm_export` script matches the encoding value assigned to the Application Server. If there is a mismatch, characters with a hexadecimal value greater than `x7F` may be corrupted during the export.

To export a scenario from the Create Scenario window, select a saved scenario from the Resources tree and click Save.

To export a scenario using an automated `cm_export` script, follow the steps in this procedure.

1. Navigate to the directory containing the `cm` export utility, typically `drive:\ibi\context\utilities\cm`, where *context* represents the folders located between the ibi root directory and the `cm` directory, and then double-click `cm_export.bat` for Windows or `cm_export.sh` for UNIX.
2. When prompted, type the ID of an administrator who is authorized to export scenarios, and then type the password for that administrator ID.
3. When prompted, type the name of the change management package you want to export.  
The utility displays the relevant parameters for this job and runs the export.
4. When prompted, press any key.

The command prompt window closes and the export process is complete.

As an alternative, you can run the export by creating a command file that contains the following parameter name values:

**USERNAME.** A WebFOCUS administrator ID.



**PASSWORD.** The password for the WebFOCUS administrator ID. If you are using a trusted authentication method, leave the password blank.

**EXPORTTO.** The name of the export folder or the name of the export package. The default name is export.

**LOGLEVEL.** Optional. The log level for the export. Possible values are:

☐ **info.** Captures only information messages. The default log level is info.

☐ **debug.** Produces maximum tracing.

**ENCODING.** Optional. A value that represents the code page used by a Change Management Export Scenario to support Java-based character encoding. In order to prevent characters with a hexadecimal value greater than x7F from being corrupted during the export, this value must match the encoding value assigned to the Application Server. The default value for this parameter is UTF-8. If your Application Server uses a different encoding value, you must replace this value with the value used by your server. For a list of client code pages and corresponding encoding value names, review the remarks in the file, cm\_export.bat.

For example, the following change management export scenario was written for the Windows operating system. It is named ACWorkspace, and it contains the USERNAME, PASSWORD, and EXPORTTO parameters and their associated values.

```
C:\ibi\WebFOCUS82\utilities\cm>type cmbatch.bat
cm_export USERNAME=admin PASSWORD=admin EXPORTTO=ACWorkspace
C:\ibi\WebFOCUS82\utilities\cm>
```

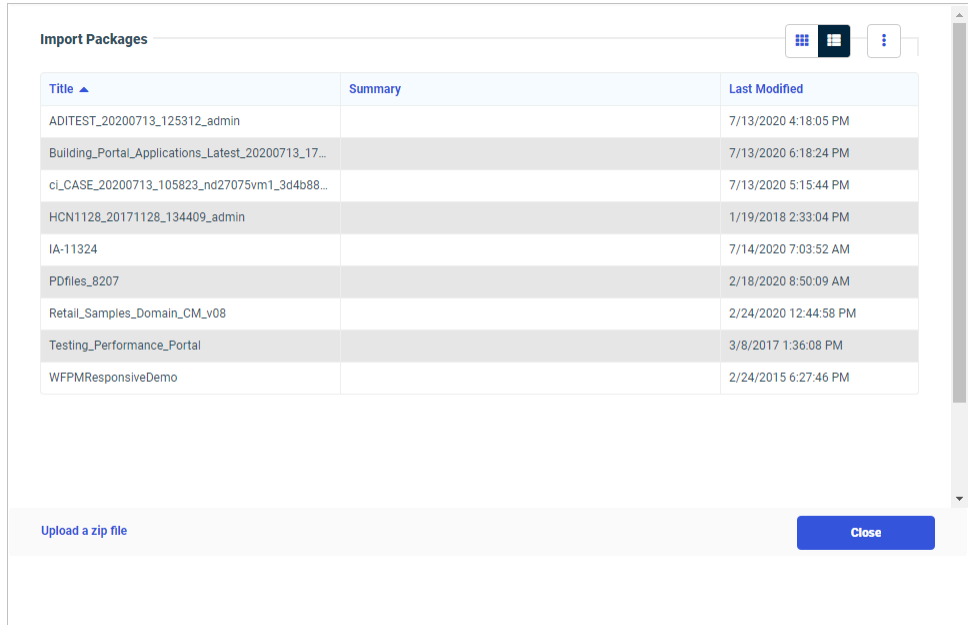
### **Procedure:** How to Upload a Change Management Package Zip File

The zip file upload process saves a copy of a CM zip file stored on your local machine to the change management import directory on the server, located at `drive:\ibi\context\cm\import`, where `context` represents the folders located between the ibi root directory and the cm directory. You can then import the copy of that CM zip file to WebFOCUS.

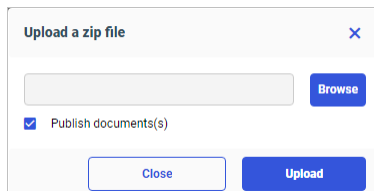
1. On the start page side navigation pane, select *Management Center* and *Import Packages*

Or

On the WebFOCUS Home Page, in the banner, open the *Utilities* menu, and select *Change Management* and *Import* to open the Import Packages dialog box, as shown in the following image.



2. Select *Upload a zip file* to open the Upload a Zip File dialog box, as shown in the following image.



3. In the Upload a Zip File dialog box, click *Browse*, navigate to the location where you have saved the change management package, click the CM zip file you want to upload, and then click *Open*.
4. Ensure that the correct CM zip file appears in the File to Upload field, and decide whether or not to import files from the package as published or unpublished files.
  - ☐ To establish the contents taken from the CM zip file as published after the upload is complete, select the *Publish Documents* check box. This is the default setting.
  - ☐ To establish the contents taken from the CM zip file as private after the upload is complete, clear the *Publish Documents* check box.

5. Click *Upload*.

A confirmation dialog box opens. Click *OK* to complete the upload.

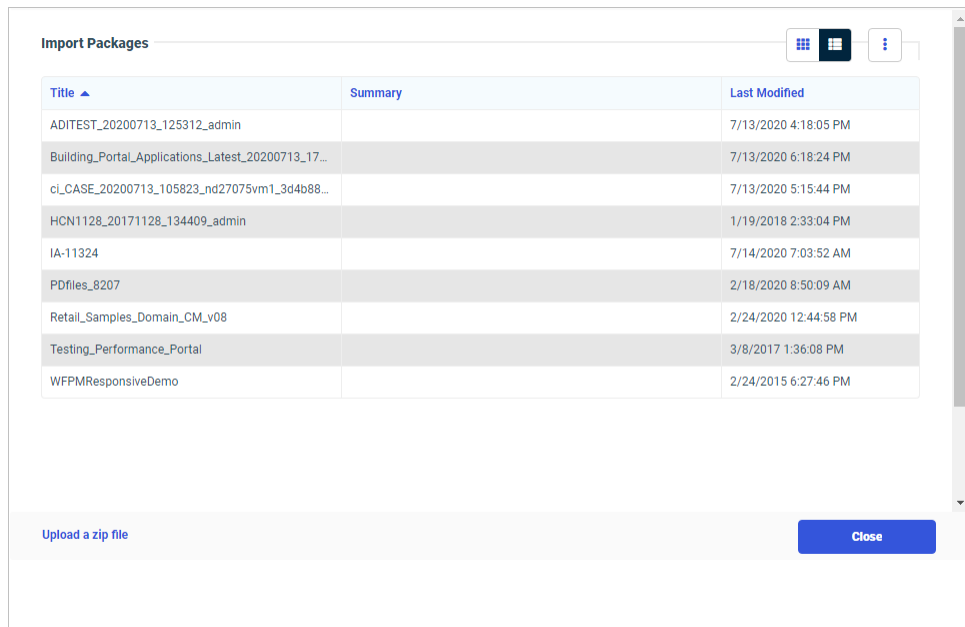
6. When you receive a message confirming that the zip file was uploaded correctly, click *OK* to complete the upload.
7. In the Upload a Zip File dialog box, click *Close*.

An entry for the new CM zip file appears in the Import Packages dialog box list.

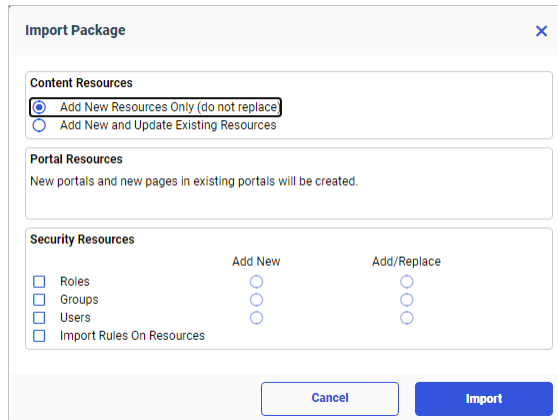
**Procedure: How to Import a Change Management Package Using the Change Management Import Facility**

1. On the start page side navigation pane, select *Management Center* and *Import Packages*
- Or

On the WebFOCUS Home Page, in the banner, open the *Utilities* menu, and select *Change Management* and *Import* to open the Import Packages dialog box, as shown in the following image.



2. Right-click the CM Zip file you want to import, and then click *Import* to open the Import Package dialog box, as shown in the following image.



The image shows the 'Import Package' dialog box. It has a title bar with a close button (X). The dialog is divided into three sections: 'Content Resources', 'Portal Resources', and 'Security Resources'. In the 'Content Resources' section, there are two radio buttons: 'Add New Resources Only (do not replace)' (which is selected) and 'Add New and Update Existing Resources'. The 'Portal Resources' section contains the text 'New portals and new pages in existing portals will be created.' The 'Security Resources' section has a table with two columns: 'Add New' and 'Add/Replace'. The rows are 'Roles', 'Groups', 'Users', and 'Import Rules On Resources'. Each row has a checkbox on the left and a radio button in each of the two columns. At the bottom, there are 'Cancel' and 'Import' buttons.

	Add New	Add/Replace
<input type="checkbox"/> Roles	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> Groups	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> Users	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> Import Rules On Resources	<input type="radio"/>	<input type="radio"/>

3. In the Content Resources group, accept the default selection, *Add New Resource Only (do not replace)*, to limit the change management import to new content resources.

or

Select *Add New and Update Existing Resources*, to enable the change management import to include updates to existing content resources as well as new content resources.

4. In the Security Resources group:
  - a. Select the *Roles* check box to include Roles in the Change Management Import package.
  - b. Select the *Groups* check box to include groups in the Change Management Import package.
  - c. Select the *Users* check box to include the individual users in the Change Management Import package.

For each security resource, accept the default selection, *Add New*, to limit the Change Management Import to new security resources.

or

Click *Add/Replace*, to enable the Change Management Import to include updates to existing security resources as well as new security resources.

- d. Select the *Rules on Resources* check box to include any new rules assigned to the security resources included in the Change Management Import package.
5. When the configuration is complete, click *Import*.

The import process loads content from the change management package into the folders that match the name and spelling of the corresponding folders in the old environment. If the resources in the change management package are assigned to the same folders and locations as in the existing environment, there are no visible changes.

However, if you do not see your expected changes, right-click the *Workspaces* entry in the Resources tree and select *Refresh*.

## Understanding Change Management Import Options

The following import options are available from the Import Package dialog box:

### Content Resources

Options in this group define the scope of content resources included in the Change Management Import. Content resources include workspaces, portals, reports, charts, and other features located under the Workspaces node and the Portals node of the Resources tree.

**Add New Resource Only (do not replace).** This option limits the import to content resources in the Change Management package that do not already exist in the target environment. The import process assigns the date and time of the import to the Created On and Last Modified On fields of all new content resources created as a result of the import. To view the Created On and Last Modified On fields, right-click an item and click *Properties*.

Resources in the change management package that already exist in the target environment are not included in the import. As a result, the resources in the target environment are not affected by the import, and the import does not update the value assigned to the Last Modified On field.

**Add New and Update Existing Resources.** This option permits the import to add new resources to the target environment and update existing resources. The import process assigns the date and time of the import to the Created On and Last Modified On fields of all new content resources created as a result of the import. The import also assigns the date and time of the import to the Last Modified on field of all existing items updated by the import, but retains the original values in the Created On field.

### Security Resources

Options in this group specify the actions to take if the change management package includes the security resources Roles, Groups, or Users. A change management package includes a security resource if it is selected explicitly, or if the *Selecting With Rules* check box is selected for another type of resource.

**Roles.** Groups of user privileges. When included in a Change Management Import package, they add to or update the list of roles maintained in the repository and visible in the Security Center on the Roles tab.

**Groups.** Collections of users or subgroups that require similar capabilities or access to the same resources. When included in a change management Import package, they add to or update the list of existing groups maintained in the repository and visible in the Security Center on the Users & Groups tab.

**Users.** Those individuals who have access to WebFOCUS. When included in a change management package, they add to or update the list of existing users maintained in the repository and visible in the Security Center on the Users & Groups tab.

For each of the Security resource categories, there are two options governing the scope of the import:

- ☐ **Add New.** This option limits the import of security resources in the Change Management package to those that do not already exist in the target environment.
- ☐ **Add/Replace.** This option permits the import to add new security resources to the target environment and update existing security resources.

**Import Rules On Resources.** This option specifies whether rules are imported from the current change management package, and is only relevant if the package contains exported rules.

As long as none of the security resource options are selected, the rules are imported using the components of the rules that exist in the target environment.

For example, if you select *Add New Resources Only (do not replace)* and *Import Rules On Resources*, the only rules that will be imported are the rules where all the components (groups, roles, and, if necessary, users) exist in the target environment.

If you select *Add New Resources Only (do not replace)* and *Import Rules On Resources*, and then select *Roles (Add New)*, the resources selected and the rules on those resources will be imported. In this case, the roles will be added only if they do not exist in the target environment and other components of the rules do exist in the target environment.

### **Procedure: How to Run a Change Management Import Scenario Using the Command-Line Interface**

You can import a scenario through the Change Management User Interface, or through an automated process executed by running one of the `cm_import` scripts, which are located in the `drive:\ibi\context\utilities\cm` directory, where *context* represents the folders located between the ibi root directory and the cm directory.

-

As part of your preparations, ensure that the code page specified by the value in the ENCODING parameter in the `cm_import` script matches the encoding value assigned to the Application Server. If there is a mismatch, characters with a hexadecimal value greater than `x7F` may be corrupted during the import.

1. Navigate to the directory containing the `cm import` utility, typically, `drive:\ibi\context\utilities\cm`, where *context* represents the folders located between the `ibi` root directory and the `cm` directory, and double-click `cm_import.bat` for Windows or `cm_import.sh` for UNIX.
2. When prompted, type the ID of an administrator who is authorized to import scenarios, and then type the password for that administrator ID.
3. When prompted, type the name of the import package.
4. When prompted, select the type of content resources to be imported. The available options are:
  - ☐ **1** to Add New Resources Only (do not replace). This is the default.
  - ☐ **2** to Add New and Update Existing Resources.
  - ☐ **Q** to quit the import process.
5. When prompted, select a role import method. The available options are:
  - ☐ **1** Skip Roles.
  - ☐ **2** Add Roles.
  - ☐ **3** Add/Replace Roles.
  - ☐ **Q** to quit the import process.
6. When prompted, select a group import method. The available options are:
  - ☐ **1** Skip Groups.
  - ☐ **2** Add Groups.
  - ☐ **3** Add/Replace Groups.
  - ☐ **Q** to quit the import process.
7. When prompted, select a user import method. The available options are:
  - ☐ **1** Skips Users.
  - ☐ **2** Add Users.
  - ☐ **3** Add/Replace Users.

☐ **Q** to quit the import process.

8. When prompted, select a Rules On Resources import method. The available options are:

☐ **1** No.

☐ **2** Yes.

☐ **Q** to quit the import process.

The utility displays the relevant parameters for this job and runs the import.

9. When prompted, press any key.

The command prompt window closes and the import process is complete.

Alternatively, you can run the import by creating a command file that contains the following parameter name values.

**USERNAME.** A WebFOCUS administrator ID.

**PASSWORD.** The password for the WebFOCUS administrator ID.

**IMPORTFROM.** Optional. The name of the import folder or the name of the import package. The default name is export.

**LOGLEVEL.** Optional. The log level for the import. Possible values are:

☐ **info.** Captures only information messages. The default log level is info.

☐ **debug.** Produces maximum tracing.

**ENCODING.** Optional. A value that represents the code page used by a Change Management Import Scenario to support Java-based character encoding. In order to prevent characters with a hexadecimal value greater than x7F from being corrupted during the import, this value must match the encoding value assigned to the Application Server. The default value for this parameter is UTF-8. If your Application Server uses a different encoding value, you must replace this value with the value used by your server. For a list of client code pages, and corresponding encoding value names, review the remarks in the file, cm\_import.bat.

**resOverwrite.** Optional. Indicates whether to import content resources. The default is not to import content resources.

**importRoles.** Optional. Indicates whether to import roles. The default is not to import roles.

**importGroups.** Optional. Indicates whether to import groups. The default is not to import groups.

**importUsers.** Optional. Indicates whether to import users. The default is not to import user.



**importRules.** Optional. Indicates whether to import rules on resources. The default is not to import rules.

For example, the following change management import scenario was written for the Windows operating system. It is named ACWorkspace, and it contains the USERNAME, PASSWORD, and IMPORTFROM parameters and their associated values.

```
C:\ibi\WebFOCUS82\utilities\cm>type cmbatch.bat
cm_import USERNAME=admin PASSWORD=admin IMPORTFROM=ACWorkspace
C:\ibi\WebFOCUS82\utilities\cm>
```



## Configuration Settings

---

This topic lists all files used to configure the WebFOCUS Client and all configuration settings in the Administration Console.

The Configuration Settings options allow you to view or edit the configuration of various components of the web application and of the WebFOCUS Client.

**In this appendix:**

- ❑ [TIBCO WebFOCUS Client Configuration Files](#)
  - ❑ [Application Settings](#)
  - ❑ [TIBCO WebFOCUS Designer Properties](#)
  - ❑ [InfoAssist Properties](#)
- 

### TIBCO WebFOCUS Client Configuration Files

The WebFOCUS Client installation creates configuration files, several of which contain settings that you can use to customize WebFOCUS for your environment. You can customize many of these files manually, but it is recommended that you use the Administration Console to edit the settings instead.

**Note:** It is strongly recommended that you update configuration settings through the Administration Console, rather than by manually editing files, whenever possible. The Administration Console automatically validates parameter values and encrypts passwords. In some cases, however, settings are read-only in the Console and can only be edited manually, because modifying those particular settings is strongly discouraged.

The following table describes the configuration files that may be customized using the Administration Console.

Installation Directory Location	File Name	Description
<i>drive:\ibi\WebFOCUS82\config</i> <i>install_directory/ibi/WebFOCUS82/config</i>	install.cfg	WebFOCUS configuration settings file. It specifies the configuration parameters selected during the initial product installation.

Installation Directory Location	File Name	Description
drive:\ibi\WebFOCUS82\config install_directory/ibi/WebFOCUS82/config	securitysettings.xml	Specifies WebFOCUS authentication methods.
drive:\ibi\WebFOCUS82\config install_directory/ibi/WebFOCUS82/config	securitysettings-mobile.xml	Specifies the authentication method for WebFOCUS mobile products, including the TIBCO WebFOCUS® Mobile App.
drive:\ibi\WebFOCUS82\config install_directory/ibi/WebFOCUS82/config	securitysettings-portlet.xml	Specifies the authentication method for WebFOCUS Open Portal Services products, including SharePoint.
drive:\ibi\WebFOCUS82\config install_directory/ibi/WebFOCUS82/config	securitysettings-zone.xml	Optionally specifies zones for multiple authentication methods.
drive:\ibi\WebFOCUS82\config install_directory/ibi/WebFOCUS82/config	webfocus.cfg	WebFOCUS configuration settings file. It specifies security changes made to the default configuration settings.
drive:\ibi\WebFOCUS82\config install_directory/ibi/WebFOCUS82/config	odin.cfg	WebFOCUS communications file. It specifies the WebFOCUS Reporting Servers to which the WebFOCUS Client can connect.  For more information, see <a href="#">TIBCO WebFOCUS Reporting Server Settings</a> on page 88.
drive:\ibi\WebFOCUS82\config install_directory/ibi/WebFOCUS82/config	mime.wfs	Contains information about available MIME types.
drive:\ibi\WebFOCUS82\client\wfc\etc install_directory/ibi/WebFOCUS82/client/wfc/etc	site.wfs	Used to define site-specific behavior for WebFOCUS script processing.

Installation Directory Location	File Name	Description
<code>drive:\ibi\WebFOCUS82\client\wfc\etc</code> <code>install_directory/ibi/WebFOCUS82/client/wfc/etc</code>	nlscfg.err	<p>Contains National Language Support (NLS) settings.</p> <p>For more information about the nlscfg.err file, see <a href="#">How to Configure National Language Support</a> on page 125.</p>
<code>drive:\ibi\WebFOCUS82\config</code> <code>install_directory/ibi/WebFOCUS82/config</code>	languages.xml	<p>Used to customize the Dynamic Language Switch settings.</p> <p>For more information, see <a href="#">Customizing the Dynamic Language Switch</a> on page 127</p>

## Application Settings

Application Settings determine the configuration and behavior of the WebFOCUS web application.

### **Procedure:** How to View or Edit Application Settings

1. In the Administration Console, on the Configuration tab, expand the *Application Settings* folder and click the node of the category of settings you would like to view or edit.

The settings appear in the main configuration pane.

2. Make the desired changes and click Save.

### **Reference:** Application Caches Settings

Settings on the Application Caches page configure the size and contents of the Data Values Cache on the Application Server. This cache contains values assigned to parameters used in Autoprompt Reports, Embedded BI Applications, or any procedure that includes the FIND parameter syntax to limit the range of available search parameter values.

These settings establish the default configuration for Data Values Cache operations in your environment. Administrators and users who have the privilege to work with the Session Viewer can temporarily override these default settings using options in the Caching list.

The Application Caches page also includes the Report Output Cache setting that establishes the use of a separate cache for report output.

### **Data Values Cache Paths to Exclude (IBI\_DATAVALUES\_CACHE\_EXCLUDEPATHS)**

Identifies the IBFS Paths to those folders or Master Files within the paths defined in the Data Values Global Cache Paths or the Data Values User Cache Paths settings whose values should be not be included in these caches.

If no IBFS Paths are defined in this setting, no data values are excluded from the individual resources or folders defined within the paths in the Data Values Global Cache Paths (IBI\_DATAVALUES\_CACHE\_GLOBALPATHS) or the Data Values User Cache Paths (IBI\_DATAVALUES\_CACHE\_INCLUDEPATHS) settings. This is the default value.

If one or more IBFS Paths are defined in this setting, data values from the individual resources or folders defined within these paths are excluded from the Global Data Values Cache and from individual User Session Caches even though the folder or directory in which they are contained is subject to caching.

Paths defined in this setting use the IBFS Path format. At a minimum, they must include the /EDA IBFS subsystem component, followed by the name of the WebFOCUS Reporting Server Node. Shorter, higher-level paths define a broad range of folders and the Master Files they contain. Longer paths that extend to a lower level define a narrower range of application folders and Master Files. Paths can extend down to the level of an individual application folder or a single Master File. Typically, this setting requires longer and more specific paths in order to identify the individual folders or Master Files that must be excluded from the paths defined in the other data cache settings.

When this setting includes multiple paths, each one must be separated by a semicolon (;) with no space following, as shown in the following example: /EDA/EDASERVE/retail\_samples;/EDA/EDASERVE/ibisamp.

IBFS Paths in this setting use the following structure. Only the first two components of the path are required. You can use the remaining components to narrow the focus of the path.

*/EDA/Node/ApplicationFolder/SubFolder1 ... SubFolderN/ResourceFolder/Resource*

where:

*EDA*

Is the EDA IBFS subsystem. This component is required for all paths. The initial slash (/) before this component is required.

*Node*

Is the name of the WebFOCUS Reporting Server node. This component is required for all paths.

*ApplicationFolder*

Is the name of the application folder that contains the resources whose data will be excluded from the data values cache.

*SubFolder1 ... SubFolderN*

Are the names of any folders underneath the application folder that connect to the end point of the path. Include as many folders as are necessary.

*Resource*

Is the end point of the path. If this is the name of a folder that contains one or more Master File resources, then data from all Master Files in the folder is excluded from the cache. If this is the name of a Master File without the .mas extension, then only data from this specific Master File is excluded from the cache.

**Data Values Global Cache Paths (IBI\_DATAVALUES\_CACHE\_GLOBALPATHS)**

Identifies the IBFS Paths to those resources whose data source values can be made available to all users without restriction in the Global Data Values Cache.

The paths defined in this setting should only identify resources that contain data that is not subject to DBA or row-level security restrictions. For calls to cache resources that contain data that is subject to these restrictions, the paths defined in the Data Values User Cache Paths (IBI\_DATAVALUES\_CACHE\_INCLUDEPATHS) setting are used.

If no IBFS Paths are defined in this setting, then no data source values are included in the Data Values Global Cache. This is the default value.

If one or more IBFS Paths are defined in this setting, then data values retrieved from the resources identified in those paths are included in the Data Values Global Cache.

Paths defined in this setting use the IBFS Path format. At a minimum, they must include the /EDA IBFS subsystem component, followed by the name of the WebFOCUS Reporting Server Node. Shorter, higher-level paths define a broad range of folders and the Master Files they contain. Longer paths that extend to a lower level define a narrower range of application folders and Master Files. Paths can extend down to the level of an individual application folder or a single Master File.

To include multiple folders or Master Files in this setting, you can use a short, higher-level path that includes a range of folders, or a series of longer and more detailed paths that identify a very specific group of folders and Master Files. If this setting must include multiple paths, each one must be separated by a semicolon (;) with no space following, as shown in the following example: /EDA/EDASERVE/retail\_samples;/EDA/EDASERVE/ibisamp.

IBFS Paths in this setting use the following structure. Only the first two components of the path are required. You can use as many of the remaining path components as you wish to narrow the focus of the path.

*/EDA/Node/ApplicationFolder/SubFolder1 ... SubFolderN/Resource*

where:

*EDA*

Is the EDA IBFS subsystem. This component is required for all paths. The initial slash (/) before this component is required.

*Node*

Is the name of the WebFOCUS Reporting Server node. This component is required for all paths.

*ApplicationFolder*

Is the name of the application folder that contains the resources from which data will be added to the data values cache.

*SubFolder1 ... SubFolderN*

Are the names of any folders in the path underneath the application folder that connect to the end point of the path. Include as many folders as are necessary.

*Resource*

Is the end point of the path. If this is the name of a folder that contains one or more Master File resources, then data from all Master Files in the folder is included in the cache. If this is the name of a Master File without the .mas extension, then only data from this specific Master File is included in the cache.

### **Data Values User Cache Paths (IBI\_DATAVALUES\_CACHE\_INCLUDEPATHS)**

Identifies the IBFS Paths to those resources whose data source values should only be made available to the individual user who retrieved the data.

The paths defined in this setting should only identify resources that contain data that is subject to DBA or row level security restrictions. For calls to cache resources that are not subject to these restrictions, the paths defined in the Data Values Global Cache Paths (IBI\_DATAVALUES\_CACHE\_GLOBALPATHS) setting are used.

If no IBFS Paths are defined in this setting, then no data source values are cached. This is the default value.

If one or more IBFS Paths are defined in this setting, then data values retrieved from all of the resources identified in those paths can be included in the Data Values User Cache for an individual user. If this setting must include multiple paths, they must be separated by a semicolon (;) with no space following, as shown in the following example: /EDA/EDASERVE/retail\_samples;/EDA/EDASERVE/ibisamp.



Paths defined in this setting use the IBFS Path format. At a minimum, they must include the /EDA IBFS subsystem component, followed by the name of the WebFOCUS Reporting Server Node. Shorter, higher-level paths define a broad range of folders and the Master Files they contain. Longer paths that extend to a lower level define a narrower range of application folders and Master Files. Paths can extend down to the level of an individual application folder or a single Master File.

To include multiple folders or Master Files in this setting, you can use a short, higher-level path that includes a range of folders, or a series of longer and more detailed paths that identify a very specific group of folders and Master Files. If this setting must include multiple paths, each one must be separated by a semicolon (;) with no space following, as shown in the following example: /EDA/EDASERVE/retail\_samples;/EDA/EDASERVE/ibisamp.

IBFS Paths in this setting use the following structure. Only the first two components of the path are required. You can use as many of the remaining path components as you wish to narrow the focus of the path.

*/EDA/Node/ApplicationFolder/SubFolder1 ... SubFolderN/Resource*

where:

*EDA*

Is the EDA IBFS subsystem. This component is required for all paths. The initial slash (/) before this component is required.

*Node*

Is the name of the WebFOCUS Reporting Server node. This component is required for all paths.

*ApplicationFolder*

Is the name of the application folder that contains the resources from which data will be added to the data values cache.

*SubFolder1 ... SubFolderN*

Are the names of any folders in the path underneath the application folder that connect to the end point of the path. Include as many folders as are necessary.

*Resource*

Is the end point of the path. If this is the name of a folder that contains one or more Master File resources, then data from all Master Files in the folder is included in the cache. If this is the name of a Master File without the .mas extension, then only data from this specific Master File is included in the cache.

**Note:** Paths to any folders or Master Files identified in the Data Values User Cache Paths setting take precedence over those identified in the Data Values Global Cache Paths setting. This means that if the same path appears in the Global Cache Path setting and the User Session Class Path setting, then data retrieved from the Master Files in that path moves into the User Session Cache, instead of the Global Cache.

**Data Values Max Cache Memory (MB) (IBI\_DATAVALUES\_CACHE\_MAXMEG)**

Defines the maximum amount of memory allocated to the Data Values Cache. This cache holds the data source values retrieved from queries to the WebFOCUS Reporting Server issued by procedures that identify their Master File sources with a two-part name in the FIND parameter syntax. These values are typically assigned to parameters used in Autoprompt Reports, Embedded BI Applications, or to any procedure that includes the FIND parameter syntax to limit the range of available search parameter values. This cache also contains the IBFS path to the Master File and the ID of the user that ran the procedure. The Data Values Cache uses memory on the machine that hosts the WebFOCUS Application Server.

This setting is assigned a value of zero (0), by default, meaning that no memory is allocated to the data values cache, and no data values are cached.

To activate the use of the data values cache, an administrator must assign a number from one (1) to five hundred (500) to this setting. A value of ten (10) megabytes can accommodate the caching requirements for most organizations.

**Report Output Cache (IBI\_REPORT\_CACHE\_ENABLE)**

Indicates whether or not report output is cached. The following values are available:

- ☐ **Off.** Report output is not cached. This is the default value.
- ☐ **On.** Report output can be cached, and the Properties dialog box on the Legacy home page displays the Report Output Cache Rule Name field.
- ☐ **Hidden.** Report output can be cached, but the Properties dialog box on the Legacy home page does not display the Report Output Cache Rule Name field.

Report output is information retrieved from the WebFOCUS Reporting Server in response to report or chart procedure queries and includes data values, column titles, and formatting features.

**Note:** The Report Output Cache Rule Name field displays a text string that identifies the rule that governs the way in which report output data is cached. These rules determine if a cache is available to everyone, available only to the user that requested the data, or if it can be shared by the members of the group to which that user is assigned.

**Procedure: How to Configure a Data Values Cache**

1. Sign in as an administrator, and then open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, click *Application Caches* to display the Application Caches page.
3. Type the number of megabytes of Application Server memory that should be allocated to the Data Values Cache in the Data Values Cache Max Memory (MB) (IBI\_DATAVALUES\_CACHE\_MAXMEG) setting. It must be a value between 0 and 500.
4. Type the paths to all resources containing data that can only be included in the individual cache assigned to the user who requested it and unavailable to others in the Data Values User Cache Paths (IBI\_DATAVALUES\_CACHE\_INCLUDEPATHS) setting.

**Note:** If you must type multiple paths in this setting or in the following settings, end each path with a semicolon (;) and leave no space between paths.

5. Type the paths to all resources containing data that can be included in the global cache and made available to anyone in the Data Values Global Cache Paths (IBI\_DATAVALUES\_CACHE\_GLOBALPATHS) setting.
6. If you must *exclude* any folders or Master Files within the paths you identified in either the Data Values Global Cache Paths setting or the Data Values User Cache Paths setting from the data values cache, type the paths to them in the Data Values Cache Paths to Exclude (IBI\_DATAVALUES\_CACHE\_EXCLUDEPATHS) setting.

This step is optional, and is not typically included in a data values cache configuration.

7. Click Save.

Your changes become effective immediately. Do not click *Clear Cache*.

**Reference: Application Contexts Settings**

Application Contexts settings define the context root locations of various WebFOCUS components.

**Help (IBI\_HELP\_CONTEXT)**

Specifies the context root for the local online Help web application.

The default value is `/ibi_help`. It is established during the product installation, and identifies the context root to which the local online Help web application is assigned, by default.

To assign the local online Help web application to the WebFOCUS context root, replace the default value with a new value that begins with the WebFOCUS Context, and is followed by the Help Context. For example, `/ibi_apps/ibi_help`.

To assign the online Help web application to any other context root, replace the default value with a new value that identifies the context root in use in your organization.

The context root defined in this setting only applies to the local host. If the Help Proxy Host and Port (IBI\_HELP\_PROXY\_HOST) setting identifies an external sever name and port, you must also identify the context root for that external server in the Help Proxy Context (IBI\_HELP\_PROXY\_CONTEXT) setting.

### **Help Proxy Context (IBI\_HELP\_PROXY\_CONTEXT)**

Specifies the context root of the remote online Help web application in the target environment identified in the Help Proxy Host and Port (IBI\_HELP\_PROXY\_HOST) setting.

This setting must remain blank if no remote online Help web application is identified in the Help Proxy Host and Port (IBI\_HELP\_PROXY\_HOST) setting. When this setting is blank, no context root is identified for the remote online Help web application. This is the default value.

This setting must identify a context root if a remote online Help web application is identified in the Help Proxy Host and Port (IBI\_HELP\_PROXY\_HOST) setting.

### **Help Proxy Host and Port (IBI\_HELP\_PROXY\_HOST)**

Specifies the name and port number of the external server where a remote online Help web application is installed.

If this setting is blank, no remote online Help web application is available. This is the default value.

If this setting contains a server name and port number, a remote online Help web application is available on the server name and port specified. The remote application does not need to be on the same server as the WebFOCUS web application.

When you specify a value in this setting, you must also specify a value in the Help Proxy Context (IBI\_HELP\_PROXY\_CONTEXT) setting. It cannot remain blank.

When you identify a remote online Help web application by assigning values to these two settings, the Help Servlet acts as a proxy, and directs Help system calls to the host identified in this setting. The term Help Proxy indicates that the values in the settings that include it apply to a remote online Help web application.

### **Help Proxy Secure (IBI\_HELP\_PROXY\_SECURE)**

If selected, this check box activates the use of Secure Sockets Layer (SSL) security on all calls directed from the WebFOCUS Client to the remote online Help web application located on the remote host identified in the Help Proxy Host and Port (IBI\_HELP\_PROXY\_HOST) setting.

If cleared, calls to the remote online Help web application, do not use SSL security or encryption. This is the default value.

**Note:** This setting does not affect calls from WebFOCUS or any other application to Help systems located on a local server. All customer-facing applications are SSL-enabled, by default, in compliance with security policy. However, if the WebFOCUS Client is configured to access a Help system on a local intranet server, this setting should be selected if the Help system on that intranet server is also configured to use SSL.

### **ReportCaster Application (IBI\_REPORTCASTER\_CONTEXT)**

Specifies the context root for ReportCaster content, previously /raster, by default. The current default value is /ibi\_apps.

### **TIBCO WebFOCUS Application (IBI\_WEBAPP\_CONTEXT\_DEFAULT)**

Specifies the context root for WebFOCUS web applications. The default value is /ibi\_apps.

### **Default host and port for product features (IBI\_WEBAPP\_DEFAULT\_URL)**

Identifies the default URL for an installation of WebFOCUS.

This value uses the format:

`http(s)://host:port`

where:

*host*

Is the name or IP address of the host used to access WebFOCUS.

*port*

Is the number of the port on which the Web Server or Application Server listens.

This value is optional, and it should be excluded if the URL uses the default port for the protocol it uses in the scheme, which is port 80 for URLs using the http protocol or port 443 for URLs using the https protocol.

The host name and the port number are assigned to this value automatically during the product installation, and they identify the host name or IP address and port number used by your organization. Product components use the URL defined in this setting to access WebFOCUS.

### **TIBCO WebFOCUS Servlet (IBI\_WEBFOCUS\_CONTEXT)**

Specifies the context root for the WebFOCUS servlet, previously /ibi\_apps, by default. The current default value is /ibi\_apps/WFServlet.ibfs.

**Reference: Application Directories Settings**

Application Directories settings define the directories in which various files are located.

**APPROOT (IBI\_APPROOT\_DIRECTORY)**

Specifies the location of the Application Namespace root directory used by the WebFOCUS installation. The default location is *drive D:/455/ibi/apps*, unless a different directory was specified during installation.

**Change Management Export (IBI\_EXPORT\_DIRECTORY)**

Specifies the location of the directory where the Change Management Export Package will be placed. The default location is *drive:/ibi/WebFOCUS82/cm/export*, unless a different directory was specified during installation.

**Change Management Import (IBI\_IMPORT\_DIRECTORY)**

Specifies the location of the directory from which the Change Management Import Package will be imported. The default location is *drive:/ibi/WebFOCUS82/cm/import*, unless a different directory was specified during installation.

**Days Until Logs Are Deleted (IBI\_LOG\_RETAIN\_DAYS)**

Specifies the number of days the files in the logs directory will be retained. The default value is 10 days.

**Directory of Source Code Staging Area (IBI\_SCM\_STAGING\_DIRECTORY)**

Specifies the location of the directory where files will be transferred during source control operations, such as adding files to source control, checking files in, or checking files out of the source control repository. The default location is *drive:/ibi/WebFOCUS82/scm*.

This location can be customized. The directory path needs to be on the same machine where WebFOCUS is installed and a UNC path is currently not supported.

**Temporary Files (IBI\_TEMPORARY\_DIRECTORY)**

Specifies the location of temporary files when running a request. For example, redirected requests are written to this location. The default location is *drive:/ibi/WebFOCUS82/temp*, unless a different directory was specified during installation.

**Traces (IBI\_TRACE\_DIRECTORY)**

Specifies the location of the directory used for WebFOCUS Client traces displayed in the Session Monitor and the Session Viewer. The default location is *drive:/ibi/WebFOCUS82/traces*, unless a different directory was specified during installation.

WebFOCUS directs all diagnostic output to the logs directory. The default location is *drive:/ibi/WebFOCUS82/logs*, specified with the log4j2.xml file during installation.

**Days Until Traces Are Deleted (IBI\_TRACE\_RETAIN\_DAYS)**

Specifies the number of days the files in the traces directory will be retained. The default value is 10 days.

**Reference: BI Portal Settings**

BI Portal settings configure the display and behavior of the BI Portal.

**Redirect /ibi\_apps to**

Identifies the default home page.

In this setting, /ibi\_apps is the main alias or context under which all WebFOCUS webpages are located. This is the typical context in most installations, but your local installation may use a different context. If that is the case, the name you use in your installation will appear in the label for this setting instead.

**Note:** Don't use the term /bi as the main alias or context. This is a reserved term, and its use as an alias or context prevents the proper display of the Administration Console and Security Center.

The options in this setting direct users to one of the following locations, by default.

- ☐ **New Start Page.** When this option is selected, the Hub, that connects you directly to WebFOCUS Client and WebFOCUS Server views from a Navigation Bar and related menus, is the default entry page. This is the default value for this setting, as of release 8207.28.
- ☐ **WebFOCUS Home Page.** When this option is selected, the WebFOCUS Home Page, first developed for Release 8.2 Version 02 is the default home page.
- ☐ **Show Legacy Home Page option in Banner Links.** Controls the display of the Legacy Home Page command in the User menu, which opens when you click your user name on the WebFOCUS Home Page. The Legacy home page was first developed in Release 8.2 Version 01. Administrators may continue to need access to this page in order to work with Resource Templates.
  - ☐ When this check box is selected, the Legacy Home Page command appears in the User menu. This is the default setting.
  - ☐ When this check box is cleared, the Legacy Home Page command does not appear in the User menu. Even if this check box is cleared, users can open the Legacy home page by typing /ibi\_apps/legacyhome in their browser address bar.

- ☐ **Legacy Home Page.** When this option is selected, the Legacy home page that was developed in Release 8.2 Version 01 is the default home page. It provides access to Global Resources, Resource Templates, and Change Management features that do not appear on the WebFOCUS Home Page.
- ☐ **Custom Welcome Page.** When this option is selected, the page that is identified in the `/ibi_apps/` field underneath this option is the default home page. Typically, a portal serves as a custom welcome page, but this setting can also contain a URL, a report, or a focexec-generated HTML page.

When you select this option, the browser address bar displays only the basic context when the custom welcome page opens. It does not display the full URL of the custom welcome page.

- ☐ **/ibi\_apps/.** Identifies the URL of the content that serves as the custom welcome page within the main alias or context.

This field contains only that portion of the URL for the custom welcome page that comes after the main alias or context. The main context is automatically added to the value in this field to create a full URL when redirecting users to the custom welcome page identified in this field.

For example, if you use a basic portal for the custom welcome page, and the full URL is:

`Server01.ibi.com:8080/ibi_apps/bip/portal/Sales_Performance.`

The value in the `/ibi_apps/` field would be:

`bip/portal/Sales_Performance.`

**Note:** You can use basic portals only if your product version supports them, and the Basic Portal option is enabled.

If you use a collaborative portal for the custom welcome page and the full URL is:

`Server01.ibi.com:8080/ibi_apps/portal/sales_october/sales_october.`

The value in the `/ibi_apps/` field would be:

`portal/sales_october/sales_october.`

**Note:** You can use collaborative portals only if your product version supports them, and the Collaborative Portal option is enabled.

If you chose to use the Portals Home Page as the custom welcome page, the value in the `/ibi_apps/` field must be:



`portals.`

**Note:** The Portals Home Page will be populated with basic or collaborative portals only if your product version supports these portal types, and the Basic Portal option and the Collaborative Portal option are enabled.

Regardless of the values you assign to this setting, users can open any home page by typing one of the following values in the browser address bar:

- ☐ To open the default home page that is defined by this setting, type `/ibi_apps`.
- ☐ To open the New Start Page, type `/ibia_apps/start`.
- ☐ To open the WebFOCUS Home Page, type `/ibi_apps/home`.
- ☐ To open the Legacy home page, type `/ibi_apps/legacyhome`.
- ☐ To open the Portals Home Page, type `/ibi_apps/portals`.
- ☐ To open a Custom Welcome Page, type `/ibi_apps/`, followed by the remaining path to the custom welcome page.

In the `webfocus.cfg` file, the Redirect `/ibi_apps` to setting maps to the `IBI_HOME_PAGE_CONFIGURATION` setting.

- ☐ When the WebFOCUS Home Page option is selected, `IBI_HOME_PAGE_CONFIGURATION=HOME`.
- ☐ When the Legacy Home Page option is selected, `IBI_HOME_PAGE_CONFIGURATION=LEGACY`.
- ☐ When the Custom Welcome Page option is selected, `IBI_HOME_PAGE_CONFIGURATION=CUSTOM`.
- ☐ When the New Start Page option is selected, `IBI_HOME_PAGE_CONFIGURATION=DEFAULT`, but because this is the default value, the `webfocus.cfg` file does not display the `IBI_HOME_PAGE_CONFIGURATION` setting.

In the `webfocus.cfg` file, the Show Legacy Home Page option in Banner Links check box maps to the `IBI_HOME_PAGE_LEGACY_LINKS` setting.

- ☐ When the Show Legacy Home Page check box is selected, `IBI_HOME_PAGE_LEGACY_LINKS=TRUE`.
- ☐ When this check box is cleared, `IBI_HOME_PAGE_LEGACY_LINKS=FALSE`.

In the webfocus.cfg file, the /ibi\_apps/ field maps to the IBI\_DEFAULT\_WELCOME\_PAGE setting.

### **Ajax Timeout (IBI\_AJAX\_TIMEOUT)**

This information is not yet available.

### **Enable Automatic Sign-out (IBI\_AUTO\_SIGNOFF)**

Activates the display of a warning message advising users that their session will expire due to inactivity, and that any unsaved work will be lost. When this check box is selected, a warning message appears on the Home Page, the Security Center, and on portals. When it is cleared, no warning message appears. This check box is selected, by default.

### **Idle Timeout Message Duration (minutes) (IBI\_AUTO\_SIGNOFF\_MESSAGE\_DURATION)**

Defines the number of minutes that a timeout warning message is displayed. This value is relevant only if the Enable Auto Sign-out (IBI\_AUTO\_SIGNOFF) check box is selected. A value of two minutes is assigned to this setting, by default.

When displayed from the Home Page or the Security Center, the warning message also identifies the time remaining until the session will end. When displayed from a portal, the warning message does not identify the remaining time.

### **Open First Workspace (IBI\_BIP\_OPEN\_FIRST\_DOMAIN)**

Determines whether the first workspace listed in the Resources tree opens automatically when you open the BI Portal. If this check box is selected (True), the first workspace opens automatically when you open the BI Portal. If this check box is cleared (False), the first workspace remains closed when you open the BI Portal. This check box is cleared, by default.

### **Concurrent Public Session Limit (IBI\_CONCURRENT\_PUBLIC\_SESSION\_LIMIT)**

Identifies the maximum number of public users that can open a session at any one time. Public users start a session without presenting credentials and are granted access privileges defined in the Anonymous group.

When the value in this setting is zero (0), there is no limit on the number of public users. This setting is assigned a value of zero (0), by default.

When a value is defined in this setting, any public user that attempts to open a session after this limit is reached receives a warning message and is unable to complete the request.

**Note:** This setting is only relevant to the Enterprise Edition, which is the only edition that supports anonymous user access.

**Concurrent Visualization Limit (IBI\_CONCURRENT\_VISUALIZATION\_LIMIT)**

Identifies the maximum number of WebFOCUS Designer or InfoAssist visualizations generated from procedures or from Auto Drill, Drill Anywhere, InfoMini, or Insight requests that a single user can keep open simultaneously. When the number of open visualizations equals this limit, the next request to open a new visualization is not completed, and an error message is logged.

This value of this setting is zero (0), by default, indicating that there is no limit on the number of simultaneous visualizations a user can open. To impose this limit, an administrator must enter a value that defines the maximum number of open visualizations.

**Customized Sign-in Page (IBI\_CUSTOMIZED\_SIGNIN\_PAGE)**

Enables the display of a custom sign-in page for users. The default value is False.

**Default Workspace Repository Path (IBI\_DEFAULT\_WORKSPACE\_PATH)**

Defines the IBFS path to the workspace that serves as the default location for connections to data, visualizations, or other resources created by individual users from the Home Page, the My Workspace view, the Getting Started carousel, or any other location outside of a defined workspace.

When a user working outside of a defined workspace selects the Get Data button, the Visualize Data button, or one of the Plus [+] button menu options, the workspace identified in this setting serves as the start location for the selected operation within the Repository, and it is presented, by default, in the Save dialog box as the location to use when first saving new content.

By default, the value in this setting is blank, and My Workspace, located at IBFS:/WFC/Repository/MyWorkspace/, serves as the default workspace repository path. This path is automatically assigned to the URL that launches the operation, and it causes the Workspaces > My Workspace > My Content path to appear in the Save dialog box as the path to the folder where new content created outside of a defined workspace can be saved.

You can replace this default location with a valid IBFS path to a different workspace or to a top-level folder in the Repository. This path is automatically assigned to the URL that launches the operation, and unless the content draws on a data connection assigned to a defined workspace, it causes the Workspaces > My Workspace > My Content path to appear in the Save dialog box as the path to the folder where new content created outside of a defined workspace can be saved.

If you enter an invalid IBFS path or a path to a workspace that does not exist, you receive an error message. The path can only point to a workspace or top-level folder, it cannot point to a lower level location.

For more information about how to configure this setting, see *Configure a Default Workspace Repository Path*.

### Notes:

- ❑ When Users working in a defined folder or workspace select the Get Data button, the Visualize Data button, or one of the Plus [+] button menu options, the path to the workspace or folder in which they are located becomes the default workspace repository path.
- ❑ Regardless of the location in which you are working when you select the Get Data button, the Visualize Data button, or one of the Plus [+] button menu options, if you select a Data Source from a defined workspace, the path to the workspace that contains your selected Data Source automatically becomes the Default Workspace Repository Path, and you are prompted to save the new resource in the workspace containing that Data Source, by default.

### Default List Repository Path (IBI\_DYNAMIC\_LIST\_PATH)

Defines the IBFS path to the workspace whose title and contents are displayed in the carousel that appears at the top of the Home view of the WebFOCUS Home Page.

A workspace whose name matches that of the final folder in the path must be present in the IBFS file system. If there is no corresponding workspace, or if the name of the workspace does not match the name of the final folder in this path, there is no connection and the carousel does not appear.

The IBFS:/WFC/Repository/Getting\_Started path is the default value for this setting. This path points to the Getting Started workspace and assigns the Getting Started title to the carousel. This default value ensures that new users see orientation resources as soon as they open the application.

The integrated installation loads the Getting Started workspace automatically. It is also present, by default, in Cloud instances. Other installations and instances of WebFOCUS do not load this workspace, even though they do assign the default path to this setting. Because there is no Getting\_Started workspace in these installations, the Getting Started carousel does not appear, even though the path to it is defined in this setting.

If a single blank space appears in the field for this setting, no path is defined, and the Getting Started carousel does not appear in the Home View even if a Getting\_Started workspace is available.

Therefore, by clearing the default value, typing a single blank space in this field, and saving your changes, you can hide the Getting Started carousel. When you sign out and sign in again after making this change, the Recents carousel appears in place of the Getting Started carousel. The blank space prevents the Administration Console from overriding the otherwise empty field with the default path when you save your changes and close the Administration Console if you opened it from the WebFOCUS Home Page.

If a path to an alternative workspace appears in the field for this setting, the carousel displays the title of that alternative workspace and the resources contained in the top-level folder of that workspace.

You can substitute an alternative workspace for the Getting Started workspace by typing the IBFS path to the alternative workspace in this field and saving your changes. When you sign out and sign in again, a carousel with the Title and resources of the alternative workspace appears in place of the Getting Started carousel.

The IBFS path must begin with the term, IBFS:/WFC/Repository. You can then type a slash (/) followed by the name of the new workspace that contains the resources you wish to display in the Getting Started carousel. You must separate workspaces and folders in the path with a slash (/) and not a backslash (\). The Title linked to the Name of the alternative workspace appears as the new title of the carousel. The name of the final folder in the IBFS path must match the case and spelling of the *Name* assigned to the workspace, not the Title. The name of the final folder must also include any underscores or other special characters automatically added to the Name of the workspace in order to ensure that it conforms to IBFS format rules.

You can restore the default value to this setting at any time by removing all characters and blank spaces from this field and saving the page. When you sign out and sign in again, the default path to the Getting Started workspace is reassigned to this setting automatically.

#### **Enable Inlined Resource Bundles (IBI\_ENABLE\_INLINED\_RESOURCE\_BUNDLES)**

This feature is optional. When selected (True), data from the JavaScript and cascading style sheet resource files, required by the WebFOCUS Home Page and WebFOCUS Designer tools, is combined into XML inline resource bundle files in order to improve system performance on slow networks. When cleared (False), this feature is not activated. This check box is cleared, by default.

**Message Detail (IBI\_MESSAGE\_DETAIL)**

Determines when users receive simplified error messages. In simplified error messages, error details can be suppressed to avoid disclosing sensitive or technical information to end users. When a simplified error message is delivered to a user, the fully detailed error message appears in the event.log to support administrator troubleshooting. Error messages in the event.log are preceded by an identifier in the form IBFS-YYMMDD\_hhmmss-*n*, where *n* is the sequence number for multiple messages generated during the same second.

The simplified error message displayed to the user contains the event.log entry identifier.

Each option in the Message Detail list specifies the highest error level for which end users will receive detailed messages. The options are:

- ☐ **Severe.** Users receive detailed messages for errors at the Severe level and below. The Severe level is the highest error level. Under this setting, users never receive simplified messages. This is the default value.
- ☐ **Error.** Users receive simplified messages for Severe-level errors, and detailed messages for errors at the Error level and below.
- ☐ **Expected.** Users receive detailed messages for Severe-level and Error-level errors, and detailed messages for errors at the Expected level and below.
- ☐ **None.** Users always receive simplified error messages.

Administrators can customize the styling of a simplified error message by creating and editing the custom template on which it is based. To create a custom error message template, copy the webfocus\_ibfs\_error.xml file from the prod directory to the custom directory. Both the prod and the custom directories are found in the `drive:\ibi\WebFOCUS82\client\wfc\etc\` directory. Make all edits to the copy of the webfocus\_ibfs\_error.xml file found in the custom directory.

**Note:** Users with the Display Administration Console (opWFAAdminConsole) or Desktop Connect (opDTConnect) privilege always receive the detailed error messages.

**Mobile Favorites Proxy URL (IBI\_MOBILE\_FAVORITES\_PROXY\_URL)**

Specifies the URL used to access Mobile Favorites. If left blank, the default Mobile Favorites is used.

**Move Confirmation Message (IBI\_MOVE\_CONFIRMATION\_MESSAGE)**

Specifies whether confirmation will be requested when a user moves a folder by drag and drop. This check box is selected (True), by default.

**Public Session Timeout (minutes) (IBI\_PUBLIC\_SESSION\_TIMEOUT)**

Controls the public session timeout value, which limits the amount of time that public users can remain idle before a session timeout takes place.

This setting is defined in minutes, and is assigned a value of 120 minutes, by default.

This setting applies to public users only. The timeout limit for all other users is defined in the Session Timeout (minutes) setting. Public users start a session without presenting credentials and are granted access privileges defined in the Anonymous group.

**Note:** This setting is only relevant to the Enterprise Edition, which is the only edition that supports anonymous user access.

**Session Privilege Search Depth (IBI\_SESSION\_PRIVILEGE\_SEARCH\_DEPTH)**

Defines how deeply searches for session privileges reach into the IBFS:/WFC/Repository subsystem during user the sign-in process. If you wish to check for session privileges only on the workspace folder, for example, IBFS:/WFC/Repository/Sales, use the default search depth, 1. To search for session privileges on subfolders directly beneath the workspace folder, use a search depth of 2.

**Note:** Search depth may be set to any level, but increasing the depth may cause performance issues. It is strongly advised that you make the search depth value as low as possible.

For more information about session privileges, see [Session Privileges](#) on page 348.

**Session Timeout (minutes) (IBI\_SESSION\_TIMEOUT)**

Controls the session timeout value, which limits the amount of time that users who signed in with valid credentials can remain idle before a session timeout takes place.

This setting is defined in minutes, and is assigned a value of 120 minutes, by default.

This setting applies to all users except public users. The timeout limit for all public users is defined in the Public Session Timeout (minutes) setting.

**Sign-in Message (IBI\_SIGNIN\_MESSAGE)**

Specifies a custom message that displays in the Messages dialog box when a user signs in. You can enter plain text or HTML tags for text, links, and images, into this field. If you leave this field blank, which is the default value, the Messages dialog box does not display.

The following HTML tags may be used in the sign-in message:

<l>, <br>, <b>, <u>, <a href>, </a>, <img>.

### **Sign-in Page Links (IBI\_SIGNIN\_PAGE\_LINKS)**

This information is not yet available.

### **Allowed File Extensions to Upload (IBI\_UPLOAD\_EXTENSIONS)**

Specifies the type of files that you can upload to the BI Portal. Files that do not use one of the extensions listed in this setting cannot be uploaded to the BI Portal. The list includes the following file extensions, by default:

.acx, .bmp, .css, .doc, .docx, .fex, .gif, .htm, .html, .ico, .jpe, .jpeg, .jpg, .js, .mas, .pdf, .png, .ppt, .pptx, .sty, .svg, .txt, .xls, .xlsx, .xml, .zip, .ely

### **Basic Default Portal Page Layout (IBI\_V3\_DEFAULT\_LAYOUT)**

Establishes the default layout for new pages in the BI Portal.

This setting is relevant only if your product version supports collaborative portals, and the Collaborative Portal option is enabled.

The default layout defined in this setting determines the way in which items, such as reports or charts, are organized on the page. Fluid Canvas, the default value, automatically arranges content evenly and redistributes space as you add more items. The other option, Single Area, does not establish a grid, and allows you to place items where necessary.

This setting is relevant only to basic portals. It is not relevant to collaborative portals.

### **Basic Portal (IBI\_V3\_PORTAL)**

Determines whether basic portals are supported.

Basic portals deliver the full range of reporting, charting, and other features, and are managed from the Portals node.

When this check box is cleared (False), the Portals node does not appear under the Resources tree, and users are unable to create or edit basic portals. However, because data from previously-created basic portals remains in the Repository, users can run a previously-created portal by typing the URL for it directly into the browser address bar. Users can also continue to import change management packages that contain basic portals. This is the default setting.

When this check box is selected (True), the Portals node appears under the Resources tree, and users can create, edit, and run basic portals.

### **Collaborative Portal (IBI\_V4\_PORTAL)**

Determines whether collaborative portals, which are also identified as V4 portals, are supported.



Collaborative portals deliver the full range of features offered by a basic portal, such as reporting and charting. They also include responsive-design page templates, the ability to create and maintain independent pages, and the ability to create and maintain blogs, which are interactive messaging components that can be assigned to portals and pages.

The check box in this setting is cleared (False), by default.

When this check box is cleared (False), the Collaborative Portal, Portal Page, and Blog action buttons in the Other tab Action Bar of the Workspaces area on the WebFOCUS Home Page, and the Collaborative Portal, Portal Page, and Blog commands in the workspace shortcut menu on the Legacy home page are not visible to any user.

Collaborative portals created while this check box was selected remain visible and available to administrators, workspace developers, and to any other user whose role in the workspace that contains them includes the Delete Resource (opDelete) privilege. The ability to view, run, edit, and delete previously-created collaborative portals supports administrators and developers in their efforts to create Designer portals, which are also identified as V5 portals, based on previously-created collaborative portals after this setting has been cleared.

When this check box is cleared, users have the following privileges as determined by the group to which they are assigned:

- ☐ **Basic Users** and **Advanced Users** cannot view or run collaborative portals.
- ☐ **Developers** cannot create collaborative portals. However, because the WorkspaceDeveloper role includes the Delete Resources (opDelete) privilege, they can view, run, edit, and delete previously-created collaborative portals within the workspaces to which they are assigned by clicking shortcut menu commands, or by typing the URL for these features directly into the browser address bar.
- ☐ **Administrators** cannot create collaborative portals. However because the SystemFullControl role includes the Delete Resources (opDelete) privilege, they can view, run, edit, and delete previously-created collaborative portals, portal pages, and blogs in any workspace by clicking shortcut menu commands, or by typing the URL for these features directly into the browser address bar. They can also export and import change management packages that contain previously-created collaborative portals, portal pages, and blogs, and can view, run, edit, or delete them after the import.
- ☐ **Note:** Previously-created portal pages and blogs also remain visible, but users with the Delete Resources (opDelete) privilege can no longer run or edit them.

When this check box is selected (True), the Collaborative Portal, Portal Page, and Blog action buttons in the Other tab Action Bar of the Workspaces area on the WebFOCUS Home Page, and the Collaborative Portal, Portal Page, and Blog commands in the workspace shortcut menu on the Legacy home page, are visible to administrators when working in any workspace, and to developers when working in the workspaces to which they are assigned.

When this check box is selected, users have the following privileges, as determined by the group to which they are assigned:

- ☐ **Basic Users** and **Advanced Users** can view and run collaborative portals made available to them.
- ☐ **Developers** can view and run collaborative portals, and they can create, edit, and delete existing collaborative portals in the workspaces to which they are assigned.
- ☐ **Administrators** can view, run, create, edit, and delete collaborative portals in any workspace. They can also export and import collaborative portals contained in Change Management packages, and they can view, run, edit, or delete them after the import.

### ***Procedure:*** How to Configure a Default Workspace Repository Path

When the Default Workspace Repository Path is blank, all content created outside of a defined workspace is assigned to My Workspace using the IBFS Path IBFS:/WFC/Repository/MyWorkspace/. Use this procedure to assign a different folder or workspace to serve as the default location for new content created outside of a defined workspace.

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, click *BI Portal* to display the BI Portal page.
3. Type the path to the workspace or top-level folder that should be used as the default location for all resources created outside of a defined workspace in the Default Workspace Repository Path (IBI\_DEFAULT\_RESOURCE\_PATH) setting.

If you receive an error message stating that your IBFS path is invalid or does not exist, retype the address and ensure that it points to an existing workspace or top-level folder.

4. Click Save.

Your changes become effective immediately. There is no need to click *Clear Cache*.

## **Reference: Change Management Settings**

Change Management settings determine which file types can be exported during the change management process, the format of the exported file, and whether some legacy functionality is preserved.

**Note:** The locations of change management export and import packages are determined by the Application Directories Settings. For more information, see *Application Directories Settings*.

### **File Types Included in Export Package (IBI\_CM\_EXPORT\_WFRS\_FILE\_EXTENSIONS)**

Determines, by file extension, which files from the WebFOCUS Reporting Server or the web will be included in exports created by the change management feature. The values included, by default, are acx, bmp, css, fex, gif, htm, html, ico, jpe, jpeg, jpg, js, mas, mnt, png, sty, and svg.

### **Preserve Created, Modified and Last Access Information (IBI\_CM\_PRESERVE\_SOURCE\_INFO)**

When this check box is selected (True), the default value for this setting, the following information is preserved for all items imported to an installation of WebFOCUS through the Change Management utility:

- ☐ **Created.** The date and time that the item was originally created, and the ID of the user who created it.
- ☐ **Modified.** The date and time that the item was most recently modified before it was added to the change management export file, and the ID of the user who made the modification.
- ☐ **Access.** The date and time that the content item was most recently used before it was added to the change management export file, and the ID of the user who used it.

These values appear on the General tab of the Properties dialog box.

When this check box is cleared (False), the date and time of the change management import and the ID of the user who ran it override these original values and are assigned to all three properties of items imported through the Change Management facility.

### **Retain Handles (IBI\_CM\_RETAIN\_HANDLES)**

When selected (True), the export package contains the original hrefs. The original hrefs are needed when using change management to move content that has been migrated from WebFOCUS 7, or ReportCaster schedules, from one WebFOCUS 8 environment to another WebFOCUS 8 environment. This setting ensures that the -INCLUDEs and drill downs in code migrated from WebFOCUS 7 continue to work, and ReportCaster schedules, which reference FOCXECs by handle, continue to work. This check box is cleared (False), by default.

### **Zip Change Management Package (IBI\_CM\_ZIP)**

When this check box is selected (True), the export package is compressed and delivered in a zip file.

### **Name format of Zip export files (IBI\_CM\_ZIP\_FILE\_FORMAT)**

Select an option from the drop-down menu to specify the name format of the zip file.

## ***Reference:* Client Settings**

Client settings configure miscellaneous WebFOCUS Client options.

### **Active Technologies external JavaScript (IBIF\_ACTIVE\_EXTJS)**

Enables the use of external JavaScript files, instead of embedding the JavaScript within the HTML output file, in order to improve performance at runtime. If set to NO, enables the use of an active report or document (format AHTML) in a fully disconnected mode that supports the browser Save As option. The default value is NO.

**Note:** For more information on the use of external JavaScript files in the HTML output, see the *Active Technologies User's Guide*.

### **DBA Source (IBIF\_DBAPASS\_SRC)**

Controls whether to pass a DBA password to the WebFOCUS Reporting Server on each request.

Permitted values are:

- ☐ **Off.** This option sets the DBA Source (IBF\_DBAPASS\_SRC) setting to blank and does not pass a DBA password with each request. This is the default option.
- ☐ **IBIMR\_user.** This option sets the DBA Source (IBF\_DBAPASS\_SRC) setting to the value of the Managed Reporting User ID.

For more information, see [DBA Password Settings](#) on page 212.

### **Excel Server URL (IBIF\_EXCELSERVURL)**

Identifies the location of the resource used to render output in the Excel 2007 file (.xlsx) format.

The Excel Server URL drop-down list contains two options:

- ☐ **DEFAULT.** Directs output to the IBIExcel Servlet on the mid tier, which will then render the output in the Excel file format. The URL used by this setting is the Default URL for the WebFOCUS mid-tier. Use this option if you do not need to support SSL or any type of authentication other than the default internal security. This is the default option.

- ☐ **Reporting Server JSCOM.** Directs output to the JSCOM3 listener on the WebFOCUS Reporting Server, which will then render the output in the Excel file format. The URL used by this setting is the URL of the JSCOM3 listener. Use this option if you need to support SSL or any type of authentication other than the default internal security.

### Graph Agents (IBIF\_GRAPHAGENTS)

Specifies the number of prestarted agents available for graph processing. The default value is 10 agents.

### Graph Server URL (IBIF\_GRAPHSEVURL)

Identifies the location of the resource used to render output in graph image file format.

The Graph Server URL drop-down list contains two options:

- ☐ **DEFAULT.** Directs output to the IBIGraph Servlet on the mid tier, which will then render the output in graph image file format. The URL used by this setting is the Default URL for the WebFOCUS mid-tier. Use this option if you do not need to support SSL or any type of authentication other than the default internal security. This is the default option.

This option is required on z/OS. In all other environments, JSCOM3 is the recommended configuration option.

- ☐ **Reporting Server JSCOM.** Directs output to the JSCOM3 listener on the WebFOCUS Reporting Server, which will then render the output in graph image file format. The URL used by this setting is the URL of the JSCOM3 listener. Use this option if you need to support SSL or any type of authentication other than the default internal security.

**Note:** If your configuration must use a different resource, contact the Customer Support Service Team to obtain assistance.

### Persistent Ampersand Variable (IBIF\_PERSISTENTAMP)

Turns on the persistent ampersand (&&) feature. By default, this check box is selected, (True). To disable this feature, clear this check box (False). The persistent ampersand feature allows you to persist && variables for the duration of the browser session.

### Do Not Add Timestamp to a Redirected Report Name (IBIWF\_AS\_NAME\_REPORT)

Determines whether a date and time are automatically removed from the end of the file name of all redirected reports using the Microsoft Excel spreadsheet format, regardless of the values assigned to the related *Redirection* setting and *Save Report* setting.

If this check box is cleared (False), the Date and Time are automatically added to the file names of redirected Excel reports. This is the default setting.

If this check box is selected (True), the Date and Time are not added to the file names of redirected Excel reports. Select this option when you must override the default system behavior and suppress the addition of a unique date and time to Excel report file names.

For information on the role of this setting in configuration with other report output redirection settings, please see [Redirecting and Saving File Output](#) on page 130.

### Default Language (IBIWF\_LANGUAGE)

With the Dynamic Language Switch feature, the default user interface language for a session is based on the language of the browser, or by setting the IBIWF\_language=*nn* parameter in the URL (where *nn* is the ISO language abbreviation).

The WebFOCUS Client uses this default setting to control the display language when the browser language of the user is not one of the available options from the Select Language drop-down list during sign-in, or if no parameter is set in the URL call.

For possible values for the ISO language abbreviations, see the *WebFOCUS National Language Support for International Computing* manual.

### Maximum Messages (IBIWF\_MAX\_MESSAGES)

Controls how many WebFOCUS Reporting Server message lines will be accumulated before WFServlet stops processing the request and displays error message 32100:

`Reporting Server messages exceeded IBIF_max_messages, report retrieval aborted.`

Messages include -TYPE commands, &ECHO=ALL variables, and errors or warnings from a data adapter. The setting protects against the situation where the Java VM executing WFServlet runs out of memory. The default value is 20000 lines. The IBIF\_max\_messages setting can be passed with the request, in which case it overrides the value set in the Console. When debug mode is enabled in App Studio, a value of 50000 is passed with each request. A value of 0 indicates that no limit exists.

### Redirection (IBIWF\_REDIRECT)

Globally sets redirection on or off. Possible values are:

- ☐ **Mime.** Respects the values set in the mime table. This is the default value.
- ☐ **Never.** Never redirects. The report output displays in the browser immediately after the request is executed. The report content is streamed to the browser without writing anything to the report cache when the content exceeds the value stored in the IBIWF\_sendbufsize setting.

- ☐ **Always.** Always redirects. The report content is saved in the temporary report cache directory. Content is moved from memory to the report cache when it exceeds the value of the `IBIWF_sendbufsize` setting. Then, a second HTTP call is made from the browser to retrieve the report content for display.
- ☐ **Length.** Does not redirect. If the size of the report content exceeds the value stored in the `IBIWF_sendbufsize` setting, the report output is moved from memory to the report cache. Once the report output is completely accumulated in the report cache, it is sent to the browser without an additional HTTP call.

### **Maximum Response Window Size (`IBIWF_REDIRENEWWINDOWSIZE`)**

Defines the maximum size, in bytes, allowed for responses in the original window when using Internet Explorer.

Responses larger than the size identified in this setting will be launched in a new window, to ensure that it will open without errors. If this setting is blank, no maximum limit is applied. The default value is 400,000 bytes.

### **Sharing cascades to (`IBI_CASCADE_SHARING`)**

Identifies the range of objects that are included when you share an unpublished procedure or object with other users. You can select one of the following options.

- ☐ **Server.** All objects referenced in a procedure or object are shared, including objects on the WebFOCUS Reporting Server. This is the default value.
- ☐ **Includes.** Only those objects referenced by `-INCLUDE` statements within a procedure or object are shared.

Referenced objects are shared in Run mode only.

When you stop sharing an unpublished procedure or object, you also stop sharing its referenced objects. However, any referenced objects shared independently of the procedure or object, remain available to their originally shared users and groups. Referenced objects assigned to multiple shared procedures or objects continue to be shared in Run mode until all of the procedures or objects in which they appear are no longer shared.

### **Google Maps API Key (`IBI_GOOGLE_MAPS_API_KEY`)**

Google API v3 does not require an API key. Therefore, this field must remain blank.

### **Google Maps API Version (`IBI_GOOGLE_MAPS_API_VERSION`)**

Determines the version number of the Google Maps™ API. Can be an integer or decimal value. An integer value represents a stable version. Currently, only Google Maps API v3 is supported.

### TIBCO Language (IBI\_LANG)

This setting is only applicable on UNIX. In order to display NLS characters on a report with server-side graphics, you must set this parameter to the appropriate UNIX locale encoding (for example, en\_US).

### Master Full Information (IBI\_MAS\_FULLINFO)

Determines if Master Files retrieved from the WebFOCUS Reporting Server include the Master File title and suffix, or not. From the drop-down menu select:

- ☐ **Default.** To conform to the setting specified in the Global Profile of the WebFOCUS Reporting Server (edasprof.prf). This is the default option.
- ☐ **Yes.** To include title and suffix from retrieved Master Files. If there are a large number of Master Files, this retrieval may be slow.
- ☐ **No.** To omit title and suffix from retrieved Master Files.

### Resource Governor Advise Messages (IBI\_RES\_GOV\_ADVISE)

Enables the display of Resource Governor advise messages for the servers you select from the list in this setting. When enabled, redirection is turned on for all report formats when the WebFOCUS Reporting Server returns any Resource Governor advise messages to display to the user. You can access the redirection settings by selecting *Redirection Settings* under the Configuration menu of the Administration Console. By default, the setting is disabled.

### Site Profile (IBI\_SITE\_PROFILE)

The following syntax enables you to include code to be executed on the WebFOCUS Reporting Server by the WebFOCUS Client.

*\_site\_profile=command*

where:

*command*

Is any valid WebFOCUS Reporting Server syntax. The site profile is not processed during a WebFOCUS Reporting Server sign-in, or when a procedure scheduled in ReportCaster is run. It is only processed when procedures are run on the WebFOCUS Reporting Server.

The site profile can also be added directly to the *drive:\ibi\WebFOCUS82\client\wfc\etc\site.wfs* file.



**Temporary File Timeout (IBI\_TEMPFILETIMEOUT)**

Deletes files from the temporary directory. Files are deleted if they are older than the number of seconds specified. The default value is 900 seconds.

**Universal Profile (IBI\_UNIVERSAL\_PROFILE)**

The following syntax enables you to include code to be executed by the WebFOCUS Client and the ReportCaster Distribution Server. This differs from the `_site_profile`, which is only executed by a WebFOCUS Client request.

`_universal_profile=command`

where:

*command*

Is any valid WebFOCUS Reporting Server syntax.

A `_universal_profile` should not include any logic or constructs that will execute only on the WebFOCUS Client. For example, http header variables should not be included, because they are available to the WebFOCUS Client, but not to the ReportCaster Distribution Server.

The universal profile can also be added directly to the `drive:\ibi\WebFOCUS82\client\wfc\etc\site.wfs` file.

**Plugin Class (IBI\_WFEXT)**

Specifies the qualified name of a plug-in class to be invoked by the WebFOCUS Servlet. By default, this variable is set to `ibi.webfoc.WFEXTDefault`, which is the default plug-in supplied with WebFOCUS that contains several useful functions.

**Transin-Transout (IBI\_WFTRANSINOUT)**

Is a fully qualified Java class that does the transin and transout processing (processing of a request to and output returned by the WebFOCUS Reporting Server) for a plug-in for the Servlet version of the WebFOCUS Client. This class must implement the `WFTransInOutInterface` Java class. For example, one use of this class can be to enable data that is passed between the WebFOCUS Reporting Server and the Servlet to be parsed for bi-directionality (left/right versus right/left strings). This setting is blank, by default.

**Reference: Deferred Reporting Settings**

Deferred Reporting settings determine how deferred reports are processed.

**Prompt for Custom Deferred Report Description  
(IBI\_DEFERRED\_CUSTOM\_DESCRIPTION)**

When this check box is selected, the default setting, users are prompted to optionally customize the description for the deferred report, which defaults to the title of the report being run deferred. This occurs whenever the description defined in the parameter (IBIMR\_defer\_description) has not been submitted with the run deferred report request.

When this check box is cleared, the title of the report being submitted to run deferred is assigned to the deferred report description automatically, and no prompt appears.

**Display Deferred Request Submitted Notification (IBI\_DEFERRED\_NOTIFY\_SUBMITTED)**

When this check box is selected, the default setting, the Deferred Request Submitted window displays to confirm a successful deferred request. The user clicks *OK* to close the window.

When this check box is cleared, the Deferred Request Submitted window does not display.

**Display Deferred Ticket Delete Confirmation  
(IBI\_DEFERRED\_TICKET\_DELETE\_CONFIRM)**

Activates an automated message that prompts the user to confirm the deletion of a deferred report. When this check box is selected, which is the default, a message prompts the user to confirm the deletion, so a deletion requires two clicks. When this check box is cleared, the user is not prompted to confirm the deletion, so a deletion requires only one click. Making a large number of deletions is faster when suppressing the confirmation message.

**Reference: Diagnostics/Tracing Settings**

Diagnostics/Tracing Settings determine specific features about system tracing and logging operations for your product installation.

**Default options for FEX tracing (IBI\_AUTO\_FEXOPTIONS)**

Establishes the default level of echo traces and SQL Traces captured from the execution of FEX file commands. In a FEX file, the &ECHO variable displays command lines as they execute, in order to test and debug procedures. The level of traces captured from all SQL request and response events. This value is set to Echo On, SQL On, by default, activating both Echo and SQL tracing for an FEX file. Administrators can override this value with any of the other setting combinations identified in the list.

**Automatic session trace level (IBI\_AUTO\_TRACE)**

Establishes the default trace level for WebFOCUS Sessions. The session trace level assigned to this setting appears, by default, in the Tracing Level list fields on the main page of the Session Viewer. Trace levels identify the level of events captured in a trace file. They range from Basic, which only captures traces of high level events, to Server, which captures traces of all events. Administrators can override this default value for individual sessions. By default, this value is set to Off, meaning that no traces are captured. For more information, see [Reviewing the Session Viewer Main Page](#) on page 187.

**Test Pages (IBI\_ENABLE\_TEST\_PAGE)**

Enables a page for testing HTTP requests and for testing RESTful web services. This check box is selected, by default. You may wish to disable this page in a production environment.

The URLs for the HTTP request test page are:

[http://host:port/context\\_root/WFServlet?IBFS1\\_action=TEST](http://host:port/context_root/WFServlet?IBFS1_action=TEST)

and

[http://host:port/context\\_root/WFServlet?IBFS1\\_action=TEST1](http://host:port/context_root/WFServlet?IBFS1_action=TEST1)

**Enable javascript error reporting (IBI\_JS\_TRACE)**

Activates the display of JavaScript error messages in the event.log file and the Session Viewer. Values in this setting are:

- ☐ **On.** Adds entries recording JavaScript errors to the event.log file and captures them in the Session Viewer and in the Session Monitor. This is the default setting.
- ☐ **Off.** Disables the logging feature. However, when using the Session Viewer, JavaScript errors are still added to traces in the Session Viewer and as entries in the event.log file.
- ☐ **Never.** Disables this feature entirely.

As a best practice, we recommend the inclusion of JavaScript errors in the event.log file and in Session Viewer traces.

### **Log all URLs when completed (IBI\_REQUEST\_LOGGING)**

Establishes the default level of URL request message logging for all sessions. All URL request log entries are posted to the requests log file, located on the Log Files page of the Diagnostic tab in the Administration Console. Administrators can override this default value for individual sessions, by selecting a different log level in the requests entry of the Log Files page. Values in this setting are:

- ☐ **Off.** Does not log URL request events.
- ☐ **On.** Logs all URL request events. Log entries for HTTP Post messages do not include data.
- ☐ **Full.** Logs all URL request events. Log entries for HTTP Post messages include data delivered with the Post request. This is the default setting.

### **Web Services SOAP Detail (IBI\_SOAP\_DETAIL)**

Displays detailed error messages in the SOAP XML response. This check box is selected, by default. If cleared, this setting suppresses details that administrators may not want to disclose to the end user.

## ***Reference:* Encryption Settings**

Encryption settings determine the encryption provider and encryption and token key locations.

### **Provider (IBI\_ENCRYPTION\_PROVIDER)**

Specifies the encryption provider used to encrypt passwords stored in WebFOCUS files. All options are based on the Advanced Encryption Standard.

The following options are supported:

- ☐ AES 128 Encryption with Internal Key  
This is the default value.
- ☐ AES 192 Encryption with Internal Key
- ☐ AES 256 Encryption with Internal Key
- ☐ AES 128 Encryption with External Key
- ☐ AES 192 Encryption with External Key
- ☐ AES 256 Encryption with External Key

If you select an option that specifies an internal key, encryption is based on a key that is embedded within WebFOCUS.

If you select an option that specifies an external key, you must create that key, assign it to a file named `key.cfg`, and save that file in the following directory:

```
drive:\ibi\WebFOCUS82\config
```

For more information about creating an external encryption key, see [Default TIBCO WebFOCUS Encryption and AES Encryption](#) on page 482.

### **Reference: ESRI Settings**

ESRI settings define the connection to the local application that supports Esri-based maps.

#### **ESRI On Premise (IBI\_ESRI\_ON\_PREMISE)**

Identifies the path to the internal ArcGIS JavaScript API Source used to develop Esri-based maps. This setting is blank, by default, meaning that the use of an internal source is not activated. To activate the use of an internal ArcGIS JavaScript API to develop Esri maps, type the path to it in this setting, typically, `/web_resource/arcgis_api`.

The default API that should be referenced by this setting is the ArcGIS API for JavaScript, version 3.28, which can be found at <https://js.arcgis.com/3.28/>. The ArcGIS JavaScript API zip file is available for download from <https://developers.arcgis.com/downloads/#javascript>. Access to this file requires a valid user ID and password which you must establish with ArcGIS.

For more information about the Esri ArcGIS Javascript API, see <https://developers.arcgis.com>.

For more information about how to configure Esri On Premise for InfoAssist, see the *Configuring an Esri On Premise Environment* topic in the *TIBCO WebFOCUS® InfoAssist User's Manual*.

For more information about how to configure Esri On Premise for App Studio, see the *Installing and Configuring Esri on Premise* topic in the *TIBCO WebFOCUS® App Studio User's Manual*.

### **Reference: Filters Settings**

Filters settings enable protections against common web security vulnerabilities.

#### **Allow Legacy WFServlet Requests, without CSRF Token (IBI\_CSRF\_ALLOW\_LEGACY)**

When selected (True). the default setting, this check box allows legacy WFServlet requests to run without requiring or using a cross-site request forgery (CSRF) security token.

### **Cross Site Request Forgery Protection (IBI\_CSRF\_ENFORCE)**

Requires all POST requests to provide a cross-site request forgery (CSRF) security token to be validated, except for legacy requests, if the exception is allowed by the IBI\_CSRF\_Allow\_Legacy setting. This check box is selected (True), by default.

### **Cross Site Request Forgery Security Token (IBI\_CSRF\_TOKEN\_NAME)**

Specifies the name of the cross-site request forgery (CSRF) security token. The default value is IBIWF\_SES\_AUTH\_TOKEN.

### **Cache Control Header (IBI\_HTTP\_RESPONSE\_HEADER\_CACHE\_CONTROL)**

Specifies the default cache control response for static content accessed by the web application. The default value is *public, max-age=2592000* (30 days). Consult Customer Support Services for assistance before altering this setting.

### **Static Content Header (IBI\_HTTP\_RESPONSE\_HEADER\_ENABLED)**

When this check box is selected (True), the default value, this setting adds the cache-control response header and the expires response header to static files that use the \*.htm, \*.html, bindowsBundle.jsp, \*.css, \*.gif, \*.png, \*.jpeg, \*.jpg, \*.txt, \*.htc, and CombinelImageServlet format.

You can modify the cache-control response header with the Cache Control Header (IBI\_HTTP\_Response\_Header\_Cache\_Control) setting. You can modify the expires response header with the Expires Header (IBI\_HTTP\_Response\_Header\_Expires) setting. However, you must consult Customer Support Services for assistance before altering this setting or either of these other settings.

### **Expires Header (IBI\_HTTP\_RESPONSE\_HEADER\_EXPIRES)**

Specifies the default expiration response header for static content served by the web application. The default value is 2592000 (30 days). Consult Customer Support Services for assistance before altering this setting.

### **Maximum content size of multipart requests (IBI\_MAX\_CONTENT\_SIZE)**

Defines the maximum size for data files uploaded to the Repository or the EDA Server. Data files that are larger than the value in this setting cannot be uploaded. The default value is 2048 megabytes. The maximum allowable value is 10240 megabytes. A value of -1 deactivates this setting.

### **RESTful Webservices Method Enforcement (IBI\_REST\_METHOD\_ENFORCE)**

When selected (True), this check box specifies that RESTful Web Services functions which create, update, or delete can only be run with the HTTP POST method.

This check box is selected, by default.

**Note:** If the Cross Site Request Forgery Protection (IBI\_CSRF\_ENFORCE) setting is set to True, then RESTful Web Services also require a CSRF token. The token name is specified with the Cross Site Request Security Forgery Token (IBI\_CSRF\_Token\_Name) setting.

#### **Maximum memory size of uploads, before cached (IBI\_UPLOAD\_MAX\_MEMORY)**

Defines the maximum amount of memory that data from files uploaded to the Repository or the EDA Server can occupy. During the upload process, data moves into memory until it reaches the limit defined in this setting. Any additional data is temporarily cached to disk. The default value is 256 megabytes. A value of -1 deactivates caching.

#### **When enabled it allows tracking of static HTML page usage (IBI\_URLFILTER)**

Information is not yet available.

#### **X-Content-Type-Options Header (IBI\_XCONTENT\_TYPE\_OPTIONS)**

When this check box is selected, an XCONTENT TYPE header is included in HTTP Response messages issued from the WebFOCUS Reporting Server. This is the default value.

By including an XCONTENT TYPE header, a server instructs the browser receiving an HTTP Response message to accept the content type assigned to the message instead of mime sniffing the data it contains and overriding the previously-assigned content type. The server asserts that the content type assigned to the message is reliable, and that the data in the message can be displayed using the content type assigned to it.

The XCONTENT TYPE header also protects the browser that receives it from cross-site scripting attacks in which mime sniffing an HTTP Response message causes a browser to execute unintended programs based on executable code hidden within its data.

When this check box is cleared, HTTP Response messages issued from the WebFOCUS server do not include the XCONTENT TYPE header, and browsers receiving it are vulnerable to cross-site scripting or other attacks. Because changing the default value assigned to this setting leaves users open to this vulnerability, we recommend that you consult Customer Support Services before doing so.

#### **Cross Site Scripting Protection Block Mode (IBI\_XSS\_MODE\_BLOCK)**

If the Microsoft Internet Explorer cross-site scripting filter is enabled in the Cross Site Scripting Protection (IBI\_XSS\_PROTECTION) setting, the value assigned to this check box specifies the response the browser makes to a cross-site scripting attack. Permitted values are:

##### ☐ **False**

If the Cross Site Scripting Protection Block Mode (IBI\_XSS\_MODE\_BLOCK) check box is clear, (False), the following value is returned:

```
X-XSS-Protection: 1
```

Internet Explorer will attempt to make minor corrections to the webpage if it detects a cross-site scripting attack. This is the default value.

☐ **True**

If the Cross Site Scripting Protection Block Mode (IBI\_XSS\_MODE\_BLOCK) check box is selected, (True), the following value is returned:

```
X-XSS-Protection: 1; mode=block
```

Internet Explorer will not render the webpage at all if it detects a cross-site scripting attack.

### **Cross Site Scripting Protection (IBI\_XSS\_PROTECTION)**

Specifies whether the Microsoft Internet Explorer cross-site scripting (XSS) filter is enabled or disabled. Valid options are:

☐ **True**

Enables the browser XSS filter by returning an HTTP response header of:

```
X-XSS-Protection: 1
```

☐ **False**

Disables the browser XSS filter by returning an HTTP response header of:

```
X-XSS-Protection: 0
```

This is the default value.

☐ **Off**

Does not return an HTTP response header to the browser. The browser relies on its default XSS filter settings for the browser security zone.

The Cross Site Scripting Protection (IBI\_XSS\_PROTECTION) setting works in conjunction with the Cross Site Scripting Protection Block Mode (IBI\_XSS\_MODE\_BLOCK) setting.

**Note:** Because application development requires HTTP requests to use characters that can be misinterpreted as a cross-site scripting attack, this filter must be disabled in a development environment. You can set Cross Site Scripting Protection (IBI\_XSS\_PROTECTION) to False (the default value) or Off. If Cross Site Scripting Protection (IBI\_XSS\_PROTECTION) is off, the browser security settings will determine if Internet Explorer invokes its cross-site scripting protection. This is required only for development purposes. If you maintain a separate production environment, you may set Cross Site Scripting Protection (IBI\_XSS\_PROTECTION) to True in that installation.



**Reference: Multiple Reports Settings**

Multiple Reports settings configure options for multi-frame reports.

**Index (IBIWF\_INDEX)**

Controls whether a sequence number is appended to the end of the names on the TOC when IBIWF\_mreports=INDEX. On appends a sequence number of 1 (for the first report generated) to *n* (for the last report generated). Off omits a sequence number. Only the text specified by the IBIWF\_mprefix setting applies. The default value is On.

**Frame Name (IBIWF\_MFRAMENAME)**

Used to name each frame in a multi-frame report. The name of each frame will be this value followed by an index number. For example, for two frames with IBIWF\_mframename set to MYFRAME, the two frames will be named MYFRAME1 and MYFRAME2. The default value is MREPORT.

**Reports Order (IBIWF\_MORDER)**

Specifies whether the report frames in a multi-frame report should appear in the order that the columns are specified in the request or the reverse order. Possible values are FORWARD and REVERSE. The default value is FORWARD.

**Prefix (IBIWF\_MPREFIX)**

Specifies up to 50 characters of descriptive text that precedes a sequence number and identifies a report in a TOC. Used to create hyperlink names in index reports. For example, if the value is *MyReport*, the hyperlinks will be composed of the name MyReport followed by an index number starting with 1. The default value is REPORT.

**Note:** Do not use this setting if IBIWF\_mreports is set to FRAME.

**Maximum Columns (IBIWF\_MRCOLUMNS)**

Specifies the maximum number of columns per page in multi-frame reports. The default value is 1 column.

**Type (IBIWF\_MREPORTS)**

Specifies whether to create an index report, a multi-frame report, or a standard report. Possible values are OFF, INDEX, and FRAME. The default value is Off.

**Maximum Rows (IBIWF\_MRROWS)**

Is the number of vertically stacked reports when the IBIWF\_mreports setting is FRAME. This setting is blank, by default.

**Reference: On-Demand Paging Settings**

On-Demand Paging settings configure On-Demand Paging options.

**Enable On Demand Paging (IBIF\_ODPENABLE)**

Controls display of On-Demand Paging (ODP) reports.

When this check box is selected (Yes), the ODP report is displayed. This check box is selected, by default.

When this check box is cleared (No), the ODP report is not displayed. Instead, a page with a message displays. You can specify the message text in the IBIODP\_disable\_msg setting. If you do not, a blank line displays.

**Disabled Message (IBIODP\_DISABLE\_MSG)**

This setting contains the message that will be displayed instead of the ODP report output when IBIF\_odpenable is set to No. The default value is a blank line (\n).

**Search Highlight HTML Tag Value (IBI\_ODP\_SEARCH\_HIGHLIGHT)**

HTML tag for highlighting text found as a result of a search in an ODP report. The default value is <u>, to underline the text.

**Target (IBI\_ODP\_TARGET)**

Controls the action of the back button in the Web Viewer.

- ☐ When this check box is selected, (On), the Back button of the browser redisplay the first ODP page. This check box is selected, (On), by default.
- ☐ When this check box is cleared, (Off) the Back button of the browser returns the browser to the calling page of the ODP report.

**Reference: OLAP Settings**

OLAP settings configure OLAP options.

These settings are visible only if the Enable OLAP check box is selected. The Enable OLAP check box appears on the Other Settings page of the Administration Console Configuration tab.

**Position (IBIF\_OLAPPOS)**

Specifies the location of the OLAP panel. Possible values are TOP and BOTTOM. The default value is BOTTOM.

**Skin Color (IBIF\_OLAPSKINCOLOR)**

Enables administrators to preview and set a new color scheme for OLAP components, such as the OLAP Control Panel. The default value is BLACK.

**Skin Name (IBIF\_OLAPSKINNAME)**

Enables administrators to create a name to preview and set a new color scheme for OLAP components, such as the OLAP Control Panel. The default value is NEUTRAL.

**Docked (IBI\_OLAP\_DOCKED)**

When the check box is selected, the OLAP Control Panel is permanently displayed while running an OLAP report. This check box is cleared, by default.

**Save Excel (IBI\_OLAP\_SAVEEXCEL)**

Specifies whether to display the OLAP *Save the data in an Excel file* option. This check box is selected, by default.

**Save Excel 2000 (IBI\_OLAP\_SAVEEXCEL2000)**

Specifies whether to display the OLAP *Save the data in an Excel 2000 file* option. This check box is selected, by default.

**Save Excel 2000 with Formulas (IBI\_OLAP\_SAVEEXCEL2000WITHFORMULAS)**

Specifies whether to display the OLAP *Save the data in an Excel 2000 file with formulas* option. This check box is selected, by default.

**Reference: Other Settings**

Other settings determine miscellaneous configuration settings.

**Legacy Cookies (IBI\_ALLOWED\_COOKIES)**

Type *WF\_USER* in this field to send this cookie back to the browser. This allows the WFSIGNON action when authenticating with the WebFOCUS Reporting Server.

**Email Server (IBI\_EMAIL\_SERVER)**

Specifies the email server used to email WebFOCUS Mobile links.

**Enable CACHECOMS (IBI\_ENABLE\_CACHECOMS)**

Activates the use of the UOA\_CACHECOMS table in background operations.

The UOA\_CACHECOMS table, located in the WebFOCUS Repository database, synchronizes multiple instances of WebFOCUS within a distributed environment by holding entries recording changes made in one instance of WebFOCUS until an internal polling process retrieves and distributes these changes to the other instances. A separate database operation polls the UOA\_CACHECOMS table and clears the table of entries that contain the previously-distributed changes once every minute.

When this check box is selected (True), the UOA\_CACHECOMS table and its related database processes are activated. This is the default value.

When this check box is cleared (False), the UOA\_CACHECOMS table and its related database processes are not activated.

You can clear this check box to suspend the use of this table and its related database operations when you need to enhance performance.

### **Enable Infographics (IBI\_ENABLE\_INFOGRAPHICS)**

Enables the use of infographics within your product installation.

When this check box is cleared, the use of infographics is disabled for everyone in the organization, including administrators and those users working with a role that includes the Display Easel.ly Link (opEaselly) privilege. By clearing this check box, administrators can override the assignment of the Display Easel.ly Link (opEaselly) privilege, and disable the use of infographics throughout their organization.

When this check box is selected, the use of infographics is enabled for administrators and for users working with a role that includes the Display Easel.ly Link (opEaselly) privilege. This is the default value.

When the use of infographics is disabled, the Utilities menu on the WebFOCUS Home Page, or the Quick Access menu on the Hub does not display the *WebFOCUS Infographics* option, eliminating the quick link to the Easel.ly website. The shortcut menu does not display the *New InfoGraphic* option, preventing users from creating new procedures based on Easel.ly template files, even if those files were downloaded directly from the Easel.ly website.

When the use of infographics is enabled, the Utilities menu on the WebFOCUS Home Page, or the Quick Access menu on the Hub displays the *WebFOCUS Infographics* option that links users directly to the Easel.ly website, where they can download Easel.ly templates that can then be uploaded to a workspace. In addition, when users right-click uploaded Easel.ly template files, the shortcut menu displays the *New InfoGraphic* option, enabling users to open Easel.ly template files and create new procedures based on them.

The Display Easel.ly Link (opEaselly) privilege is typically available to administrators and to users assigned to the Advanced User or Developer groups within a workspace.

**Note:** The value in the *Enable Legacy Features (IBI\_ENABLE\_LEGACY\_FEATURES)* setting takes priority over the value in this setting. Therefore, both the *Enable Infographics* check box *and* this check box must be selected in order to make infographics available.

### **Enable Legacy Features (IBI\_ENABLE\_LEGACY\_FEATURES)**

Enables the use of legacy features.

When this check box is cleared (FALSE), legacy feature privileges are not available and cannot be assigned to groups. This is the default setting for the cloud-based free trial installation.

When this check box is selected (TRUE), legacy feature privileges are available and can be assigned to groups. This is the default setting for all installations other than the cloud-based free trial.

The following legacy feature privileges are affected by this setting:

- ☐ Advanced Reporting Privilege Category
  - ☐ Create Alerts (opAlertAssistant)
  - ☐ Data Visualization From Metadata (opVisualization)
  - ☐ Display Easel.ly Link (opEaselly)
  - ☐ Express Analytics (opExpressAnalytics)
  - ☐ InfoAssist From Metadata (opInfoAssist)
  - ☐ InfoAssist From Reporting Object (opInfoAssistviaReportingObject)
- ☐ Application Development Privilege Category
  - ☐ Create Reporting Objects (opReportingObject)

When these legacy privileges are enabled, InfoAssist, the Reporting Object Tool, the WebFOCUS Infographics menu option, and other legacy tools are available to administrators and to users working in the Advanced Users group, the Developers group, and any group whose roles include these privileges.

**Note:** The value in this setting takes priority over the value in the *Enable Infographics (IBI\_ENABLE\_INFOGRAPHICS)* setting. Therefore, both this check box and the *Enable Infographics* check box must be selected in order to make infographics available.

### Enable OLAP (IBI\_ENABLE\_OLAP)

Enables OLAP settings and functionality. When this check box is selected, OLAP functionality appears in the following locations:

- ☐ **WebFOCUS.**
  - ☐ In the Security Center, Basic Reporting section: Run Procedures with OLAP permission.
  - ☐ On the Administration Console, Configuration Tab: OLAP Settings page.
  - ☐ In the Properties dialog box: Run with OLAP check box.

**Note:** In the Properties dialog boxes of portals and workspaces, this check box appears dimmed and is unavailable. In the Properties dialog boxes of reports, charts, and visualizations, this check box is fully visible and available.

- ☐ **InfoAssist and InfoAssist Basic.** On the Auto Drill and Analysis menu: All OLAP-related features including the OLAP Options panel, OLAP panel, OLAP Ribbon, and OLAP Reports.

This setting does not activate the use of OLAP within App Studio. To do so, open App Studio, and select the Enable OLAP check box on the Reporting tab of the App Studio Options dialog box. For more information, see the *Setting User Preferences Using the Options Dialog Box* topic in the *WebFOCUS App Studio User's Manual*.

This check box is cleared, by default.

#### **User Default Roles (Used For Migration) (IBI\_ENABLE\_UDR)**

For migrated environments, enables the Default Role tab in the Security Center. This check box is cleared, by default.

#### **Excluded File Extensions for Reporting Server (IBI\_EXCLUDE\_WFRS\_FILE\_EXTENSIONS)**

Identifies the type of files that cannot be uploaded to the WebFOCUS Reporting Server. Files types are identified by their extension. For example, PDF files that use one of the extensions listed in this setting cannot be uploaded. This setting is blank, by default, enabling you to upload any type of file.

#### **Convert FOCUS Errors to Warnings (IBI\_FOCUS\_WARNING\_NUMBERS)**

Contains one or more FOCUS error message numbers separated by commas. WebFOCUS and ReportCaster regard the FOCUS error messages whose numbers appear in this setting as warnings instead of error messages.

If WebFOCUS encounters one of these FOCUS error message numbers, it generates a warning message instead of an error message and does not highlight the trace that captures the FOCUS error message as an error in the Session Viewer.

If ReportCaster encounters one of these FOCUS error message numbers when executing a report schedule, it distributes the report in spite of the FOCUS error message, and does not trigger an error notification, even if the report schedule is configured to use the *On Error* Notification Type.

#### **Paths to Item Descriptions to be Indexed (IBI\_INDEX\_DESCRIPTION)**

Identifies the paths to those folders in which item descriptions are indexed for the Magnify Search engine.

When the term OFF appears in this setting, item description indexing is deactivated. This is the default value.

When one or more paths appear in this setting, item description indexing is activated for all items within the final folder identified in each path. Whenever an item within a folder identified by one of the paths in this setting is created, or the description or summary of an existing item within that folder is modified, the description and summary of that item are indexed automatically. If the final folder in a path includes multiple folders, item description indexing is activated for all of them.

Paths follow the IBFS path format. For example:

```
/wfirs/ibfs/WFC/Repository/Retail_Samples/Reports/
```

Multiple paths must be separated with a semicolon (;).

### **Enable InfoSearch (IBI\_INFOSEARCH)**

When this check box is selected, the Display Ask TIBCO WebFOCUS Menu (opInfoSearch) privilege is available in the Security Center Roles dialog box, making InfoSearch available to users. This is the default value for this setting.

When this check box is cleared, the Display Ask TIBCO WebFOCUS Menu (opInfoSearch) privilege is removed from the Security Center Edit Role dialog box, making InfoSearch unavailable to users.

After a new product installation or upgrade, this check box is selected, by default, making InfoSearch and the Display Ask TIBCO WebFOCUS Menu (opInfoSearch) privilege available automatically. However, even when this check box is selected, the text-based search capability it enables becomes available only when users have the Display Ask TIBCO WebFOCUS Menu (opInfoSearch) privilege and dimensionally-indexed Repository content is available.

Because clearing this check box also hides the Display Ask TIBCO WebFOCUS Menu (opInfoSearch) privilege, administrators should not clear this check box unless they intend to remove the ability to use InfoSearch from all users. To re-establish this setting, an administrator must select the Enable InfoSearch check box again.

**Note:** InfoSearch is a search tool that retrieves content items in the Repository that contain data or metadata that matches the words or expressions used in the search query. It is a superset of the Magnify Search tool, and InfoSearch is purchased separately. Customers that purchase Magnify Search, but not InfoSearch, will be able to use the InfoSearch Retail Samples demo, but they will not be able to use InfoSearch with any other data or content.

### **Library Item Default Action (IBI\_LIBRARY\_ITEM\_DEFAULT\_ACTION)**

Determines whether double-clicking a library item opens the latest version of the report (*Last*) or a list of report versions (*Versions*). The default value is Last. The value you specify here appears first in the shortcut menu when you right-click a library item and click *View*.

### **Enable Mobile Voice (IBI\_MOBILE\_VOICE)**

This check box is visible only if the license key for your installation includes the TIBCO WebFOCUS Mobile product component.

When this check box is selected, the Display Ask TIBCO WebFOCUS for Mobile Voice (opMobileVoice) privilege is available in the Security Center Roles dialog box, making the Mobile Voice interface available to all users. This is the default value for this setting.

When this check box is cleared, the Display Ask TIBCO WebFOCUS for Mobile Voice (opMobileVoice) privilege is removed from the Security Center Roles dialog box, making the Mobile Voice interface unavailable to all users.

After a new product installation or upgrade that includes a license for the TIBCO WebFOCUS Mobile product component, this check box is visible and selected, by default, making Mobile Voice and the Display Ask TIBCO WebFOCUS for Mobile Voice (opMobileVoice) privilege available automatically.

However, even when this check box is selected, Mobile Voice search capability becomes available only when licensed users are working with a role in which the Display Ask TIBCO WebFOCUS for Mobile Voice (opMobileVoice) privilege is selected, dimensionally-indexed Repository content is available, and at least one Intent phrase has been defined for an available resource.

Because clearing this check box also hides the Display Ask TIBCO WebFOCUS for Mobile Voice (opMobileVoice) privilege, administrators should not clear this check box unless they intend to remove the ability to use Mobile Voice from all users. To re-establish this setting, an administrator must select the Enable Mobile Voice check box again.

### **Prompt for Connection Credentials Option (IBI\_PROMPT\_FOR\_CONNECTION\_CREDENTIALS)**

When this check box is selected (True), the Run Procedures with Different Connection Credentials (opRunAs) privilege becomes available in the Basic Reporting privilege category of the Roles dialog box.

Users who are granted this privilege can select the *Run with different connection credentials* option from the shortcut menu. This menu option allows users to provide credentials when running procedures against databases that require additional authentication against their internal credentials in order to provide access to an elevated data set. It extends reporting capabilities to information that would otherwise be unavailable without the ability to authenticate alternative user IDs and passwords at runtime.

When this check box is cleared (False), neither the privilege nor the menu option is available. This is the default value for this setting.



This setting only affects the configuration of the *Run with different connection credentials* menu option within the WebFOCUS Client. In order to complete the configuration of this functionality, the WebFOCUS Reporting Server and individual database connections must also be configured to accept the use of additional credentials. For more information about the WebFOCUS Reporting Server configuration, see the *TIBCO WebFOCUS® Reporting Server Administration* technical content.

For more information about the WebFOCUS Client configuration, see *Configuring Run With Different Connection Credentials*.

### **Upload Images to be Embedded in Reports (IBI\_PUSH\_IMAGE)**

Uploads Repository images to the WebFOCUS Reporting Server for embedding in reports and HTML pages. This check box is selected, by default.

### **Custom Strings (IBI\_RESOURCEBUNDLE\_ALTERNATE\_PREFIXES)**

The name of the file that contains text strings used to customize labels for global items, such as menu bar options, error messages, and other features. This field is blank, by default.

**Note:** Consult Customer Support Services before modifying this setting.

### **Paths to be executed on user Sign-in (IBI\_SIGNIN\_PATHS)**

Lists all procedures that run when users sign in to a portal or to web services. By default, this setting is blank, and no procedures run in response to user sign in. To configure a list of procedures, type the path name for each of them in this setting, and separate each path name with a comma, as shown in the following example.

```
IBFS:/WFC/Repository/Public/motd.fex,
```

The procedures you include in this setting can serve a variety of purposes. For example, you can use this setting to run a procedure that sends a message of the day to users upon sign-in, using the syntax shown in the following example of the message of the day file, motd.fex.

```
-IF &FOCSECUSER EQ admin GOTO ADMINMSG;
-TYPE <UserMsg>Hello normal user</UserMsg>
-GOTO DONE;
-ADMINMSG
-TYPE <UserMsg>Hello admin</UserMsg>
-DONE
```

You could also use this setting to run a procedure that initializes the environment and establishes a procedure within the repository that creates a single foccache ticket that can be used for all subsequent requests, as shown in the following example.

```
TABLE FILE IBISAMP/CAR PRINT COUNTRY  
IF RECORDLIMIT EQ 1  
ON TABLE HOLD AS FOCCACHE/LATCH  
END
```

This procedure cannot produce any report output.

### **Technical Preview Features (IBI\_TECHPREVIEW\_FEATURES)**

Activates the technical preview mode, which enables users to view and evaluate specific features planned for an upcoming release.

This setting is relevant only to product versions that include preview features. Because each release contains a different set of new features, the code names of preview features for one version may not be relevant to another version. Therefore, lists that do not contain the code name of any feature that appears in the technical preview mode of the version that is currently installed, fail to activate the technical preview mode.

When this setting is blank, the technical preview mode is not activated, and users are not able to preview new features. This is the default value.

When this setting contains a semicolon-delimited list of the code names of one or more of the features that are included in the technical preview mode of the version of the product that is currently installed, WebFOCUS activates the technical preview mode, and users can open and test the new features included in the list.

When the technical preview mode is activated, administrators receive a message identifying the technical preview features that are currently enabled immediately after sign-in. This message is also posted to the event log along with other records of the administrator sign-in event. No other users receive this message after sign-in.

### **Override for Tools Theme (IBI\_TOOL\_THEME)**

Identifies the name of the theme assigned to InfoAssist and Business Intelligence Portal designer tools. This value is blank, by default, meaning that the default theme behavior is in effect for these tools. The other value, BIPNeutral, sets the default theme for these designer tools to a more modern and neutral appearance.

## Configuring Run With Different Connection Credentials

The *Run with different connection credentials* menu option opens connections to databases that support the authentication of different credentials that are maintained within the database targeted by a procedure. Typically, databases that support the use of different credentials contain information that can only be made available to users who can present these credentials at runtime. These different credentials supplement the access to generally available information provided by the default service account credentials used to authenticate the connection to data.

Configuration features within the WebFOCUS Reporting Server browser interface and within the WebFOCUS Client enable administrators to make this menu option and functionality available to users on a scale that conforms to the requirements of their organization.

Within the WebFOCUS Reporting Server, the ability to use different connection credentials can be assigned only to those database connections that require it.

Within the WebFOCUS Client, the ability to run a procedure that requires different connection credentials can be assigned only to those content resources that require access to databases that maintain their own credentials, and then only to those users who are authorized to use different credentials with those databases.

To ensure that the Run Procedures with Different Connection Credentials privilege is available only to those users who need it when working with resources that support the use of different connections, you must establish the following configuration in the WebFOCUS Client:

1. Ensure that the WebFOCUS Reporting Server is configured to support different connection credentials for those database connections that require it.

For more information about the WebFOCUS Reporting Server configuration, see the *TIBCO WebFOCUS® Reporting Server Administration* technical content.

2. Select the *Prompt for Connection Credentials Option* check box, located on the Other Settings page of the Administration Console Configuration tab, in order to make the Run Procedures with Different Connection Credentials (opRunAs) privilege available for roles.

For more information, see *Activate the Prompt for Connection Credentials Option Setting*.

3. Assign the Run Procedures with Different Connection Credentials (opRunAs) privilege, located in the Basic Reporting privileges category of the Roles tab in the Security Center, to those roles that will be assigned to groups who need to use this menu option.

For more information, see [How to Edit a Role](#) on page 468. If you wish to create a new role that includes this privilege, see [How to Create a Role](#) on page 467.

4. Ensure that users who need to use this menu option are assigned to the groups that include this privilege.

If you need to assign users to the groups that will use this privilege, see [How to Add a User to a Group](#) on page 460.

5. Create rules for all content items that support the use of different credentials by assigning roles containing the Run Procedures with Different Connection Credentials (opRUNAs) privilege to those groups whose members are entitled to enhanced user access when running those items.

For more information, see [How to Create a Rule on a Content Resource](#) on page 470.

### **Procedure:** How to Activate the Prompt for Connection Credentials Option Setting

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, select *Other Settings* to display the Other Settings page.
3. Select the *Prompt for Connection Credentials Option* check box.
4. Click Save.
5. When you receive a message stating that your changes were saved successfully, click OK.
6. From the Administration Console Menu bar, click *Clear Cache*.
7. When you receive a message that the cache was cleared successfully, click OK.
8. Sign out of your current session.
9. Sign in again to continue the configuration.

### **Reference:** Parameter Prompting Settings

Parameter Prompting settings determine parameter prompting behavior in the WebFOCUS Client.

#### **Null Behavior (IBIF\_DESCRIBE\_NULL)**

Specifies the value (\_FOC\_NULL or FOC\_NONE) that the WebFOCUS Client assigns (in a -SET command) to the amper variable when the dynamic multi-select list *No Selection* value is selected. The default value is \_FOC\_NULL.

#### **Managed Reporting (IBIMR\_PROMPTING)**

Enables or disables parameter prompting for all Managed Reporting requests. Possible values are:

- ☐ **Off.** Turns off parameter prompting at the site level.
- ☐ **Run with Default Values (XMLRUN).** Prompts for amper variables that were created with the -DEFAULT command and any other amper variable that does not have a value.

- ☐ **Always Prompt (XMLPROMPT).** Prompts for amper variables that were created with the -DEFAULT command when there is another amper variable that does not have a value assigned. This is the default value.

### **Managed Reporting when Prompt Parameters Property Unset (IBIMR\_PROMPTINGUNSET)**

Enables or disables parameter prompting for Managed Reporting procedures (FEXes) when Managed Reporting (IBIMR\_PROMPTING) is set to Always Prompt (XMLPROMPT) or Run with Default Values (XMLRUN), and the Prompt for Parameters check box is unselected in the FEX Properties dialog box. Possible values are:

- ☐ **Off.** Turns off parameter prompting.
- ☐ **Run with Default Values (XMLRUN).** Prompts for amper variables that were created with the -DEFAULT command and any other amper variable that does not have a value. This is the default value.
- ☐ **Always Prompt (XMLPROMPT).** Prompts for amper variables that were created with the -DEFAULT command when there is another amper variable that does not have a value assigned.

### **Auto Describe (IBI\_AUTODESCRIBE)**

Activates automatic indexing of report and chart parameters. If this check box is selected (True), when users save reports or charts, the parameters on which they are based are indexed automatically, making information about these parameters immediately searchable, and delivering more timely and comprehensive search results.

This check box is selected (True), by default.

### **Default Autoprompt Template (IBI\_DESCRIBE\_TEMPLATES)**

Specifies the template that defines the layout of the autoprompt interface.

- ☐ **Designer.** Specifies the use of the Designer Autoprompt implementation and the Designer Autoprompt template. In this template, the Autoprompt interface uses the Designer page format. This is the default value.
- ☐ **Responsive.** Specifies the use of the responsive implementation and the autoprompt\_jqm.jsp template.
- ☐ **HTML\_Top.** Specifies the use of the HTML-based implementation and the autoprompt\_top.html template, which displays parameters horizontally at the top of the page.

- ☐ **HTML\_Top\_Checked.** Specifies the use of the HTML-based implementation and the `autoprompt_top_checked.html` template. In this template, the Run in a new window check box is pre-selected, specifying that all reports open in a new window, by default.

You can add customized versions of HTML and Responsive autoprompt interface templates to this list by typing template name tags for them in the `aptemplates.xml` file. However, the Designer autoprompt interface template is not available for customization. For more information, see *Add Custom Autoprompt Templates* and *Test Custom Autoprompt Templates*.

### **Preselect all values for static list controls (IBI\_FOCALL\_DEFAULT)**

Activates the automatic selection of all values in Responsive Autoprompt multiselect static selection list parameters at runtime, by default.

If this check box is selected (True), Responsive Autoprompt selection list parameters that contain multiselect static lists are automatically assigned `FOC_ALL` as their initial selection value, by default, causing these lists to automatically display all values as selected at runtime. However, if a multiselect static list designates a default value for display, that value overrides the automatic assignment of `FOC_ALL` as the initial selection value, and that default value is displayed as the initial selection instead.

If this check box is cleared (False), parameters that contain multiselect static lists are not automatically assigned `FOC_ALL` as the initial selection value, by default, and all items within the list are not selected automatically at runtime. If a multiselect static list contains a designated default value, that value is displayed, by default. To include all values from the static selection list in a query, a user must manually select the All Values option or individually select all values in the list.

This check box is cleared (False), by default.

### **Self Service (IBI\_WFDESCRIBE\_DEFAULT)**

Enables or disables amper auto prompting for self-service reporting. Possible values are:

- ☐ **Off.** Turns off auto prompting. This is the default value.
- ☐ **Run with Default Values (XMLRUN).** Prompts for amper variables that were created with the `-DEFAULT` command and for any other amper variable that does not have a value.
- ☐ **Always Prompt (XMLPROMPT).** Only prompts for amper variables that were created with the `-DEFAULT` command when there is another amper variable that does not have a value assigned and, therefore, will be prompted for.

- ☐ **Display XML (Debug with syntax error checking) (XML).** Displays the XML document describing the amper variables in the browser. This setting is used internally, and is recommended for debugging and syntax error checking purposes only.
- ☐ **Display XML (Debug) (XMLCHECK).** Displays the XML document describing the amper variables in the browser. This setting is used internally, and is recommended for debugging purposes only.

**Note:** Managed Reporting uses a separate variable setting, which is IBIMR\_PROMPTING.

### **Procedure:** How to Add Custom Autoprompt Templates

This procedure describes how to add entries for custom autoprompt interface templates directly into the `aptemplates.xml` file. These custom templates appear in the Default Autoprompt Template (IBI\_DESCRIBE\_TEMPLATES) setting list in addition to the three templates loaded there, by default. For additional information about the template name tag and its attributes, see the comment section at the top of the `aptemplates.xml` file.

1. On the machine where WebFOCUS is installed, navigate to `drive:\ibi\WebFOCUS82\client\wfc\etc\prod`.
2. Copy the `aptemplates.xml` file from the `\prod` folder to the `\custom` folder located in the `\etc` directory.
3. In the `\custom` folder, open the `aptemplates.xml` file with a text editor, and scroll to the end of the file.
4. Place the cursor after the `<APTemplates>` tag.
5. Add a custom template by typing a `<template>` tag that contains the following attributes:

```
<template name="templatename" src="templatepath" type="{HTML/REDIR}" />
```

where:

*templatename*

Is the name of the custom template to display in the Default Autoprompt Template list. For example: `template name="RedirectTemplate"`.

*templatepath*

Is the path name and file name of the custom template. Custom autoprompt template files must only be added to one of the following WebFOCUS folders:

- ☐ **Responsive autoprompt templates.** `drive:/ibi/WebFOCUS82/webapps/webfocus/tools/autoprompt_jqm`
- ☐ **HTML-based autoprompt templates.** `drive:/ibi/WebFOCUS82/ibi_html/javaassist/ibi/html/describe`

**Note:** The Designer autoprompt template is not available for customization.

*type*

Is the autoprompt implementation type.

*HTML*

Specifies that the template is used for the HTML implementation.

*REDIR*

Specifies that the template is used for the Responsive implementation.

For example:

```
<template name="HTMLhorizontal" src="C:/ibi/WebFOCUS82/ibi_html/
javaassist/ibi/html/describe/autoprompt_top.html" type="HTML" />
```

6. Repeat the previous step for all of the additional custom autoprompt interface templates that you want to add to the aptemplates.xml file.
7. When you have added tags for all custom autoprompt interface templates, save the file.
8. Sign in as an administrator, and open the Administration Console.
9. In the Administration Console Menu bar, click *Clear Cache*.
10. When you receive a message stating that the individual caches are clear, click OK.
11. Test the updates. For more information, see *Test Custom Autoprompt Templates*.

### ***Procedure:*** How to Test Custom Autoprompt Templates

1. On the Configuration tab, under the Application Settings folder, click *Parameter Prompting*.
2. On the Parameter Prompting page, click the *Default Autoprompt Template* list.
3. Review the list to confirm that it includes the custom templates added to the aptemplates.xml file.
4. If one or more custom templates are not listed, open the aptemplates.xml file and review the <template name> tags to confirm that the attributes and values are specified correctly for each one. For more information, see steps 5 - 7 in *How to Add custom Autoprompt Templates*.
5. When entries for all custom templates appear in the list, select one of them, and then click *Save*.
6. When you receive a message stating that the changes were saved successfully, click *OK*.
7. Select or create a report request that includes filter parameters with no assigned values, and has selected the Prompt for Parameters property check box.
8. Run the selected report request to determine if it displays the custom Autoprompt page you selected in step 5.



9. If the custom autoprompt interface you selected in step 5 does not appear, there may be an error. Review browser traces and WebFOCUS Client Session traces to identify any errors.
10. If the custom autoprompt interface you selected in step 5 appears, close the request.

**Reference: Quick Data Settings**

Quick Data settings determine how Quick Data performs authentication.

**Form Only (IBI\_QUICK\_DATA\_FORM\_ONLY)**

Applies when MR authentication is selected for the IBI\_Quick\_Data\_Security setting. Permitted values are

- ☐ **Yes.** Users may not create their own reports using InfoAssist, but may only use predefined ad hoc forms.
- ☐ **No.** Users may use predefined ad hoc forms or create their own reports, using InfoAssist. The default value is No (clear check box).

**Security (IBI\_QUICK\_DATA\_SECURITY)**

Specifies the type of sign-in used by WebFOCUS Quick Data. Permitted values are *Reporting Server* and *Managed Reporting*. The default value is *Reporting Server* and requires no additional configuration.

**Reference: Repository Settings**

Repository settings specify the authentication credentials that the JDBC driver uses to access the Repository.

**Effective Policy Cache Limit (IBI\_CACHE\_EFFECTIVE\_POLICIES\_PER\_SESSION\_LIMIT)**

Specifies the maximum number of security policies retained for a single session. The default value is 50 policies and the maximum value is 500 policies.

**Effective Policy Cache Duration (IBI\_CACHE\_EFFECTIVE\_POLICY\_DURATION)**

Specifies the duration, in minutes, that a cached security policy is considered valid. The default value is 180 minutes and the maximum value is 720 minutes.

**User Name Cache Limit (IBI\_CACHE\_USERNAMES\_LIMIT)**

This information is not yet available.

**External Group Cache Duration (IBI\_CACHE\_USERS\_EXTERNAL\_GROUPS\_DURATION)**

Specifies the duration, in minutes, that the list of external groups for each user will be retained. The default value is 180 minutes and the maximum value is 720 minutes.

**External Group Cache Limit (IBI\_CACHE\_USERS\_GROUPS\_LIMIT)**

Specifies the number of users for whom to retain the list of group memberships. The default value is 50 users and the maximum value is 1000 users.

**User Profile Cache Duration (IBI\_CACHE\_USER\_AFTER\_SIGNOFF\_DURATION)**

Specifies the number of minutes that user security information will be retained after sign-out. The default value is 30 minutes.

**Note:** This setting may be useful for applications that run web services applications that sign in, perform a minor task, and sign out.

**Procedure Cache Limit (IBI\_CACHE\_WFC\_FEX\_LIMIT)**

Specifies how many procedures (.fex files) are cached in memory to improve response time. The default value is 100 procedures (.fex files).

**Synchronization Interval (IBI\_REPOSITORY\_SYNC\_INTERVAL)**

Specifies, in minutes, the interval at which other JVMs will synchronize security information with the Repository, when multiple JVMs are using the same repository. For example, security information is not updated in the other application servers in a cluster or in the ReportCaster Distribution Server until this interval elapses. The default value is 1 minute.

**Database Driver (IBI\_REPOS\_DB\_DRIVER)**

Specifies the Java Database Connectivity API (JDBC) driver used to access the Repository.

The value in this setting is not available for updates. If you must change the default value assigned to this setting, contact the Customer Services Support team.

**Database Password (IBI\_REPOS\_DB\_PASSWORD)**

Specifies the password used by the JDBC driver to access the Repository.

**Database URL (IBI\_REPOS\_DB\_URL)**

Specifies the URL used by the JDBC driver to access the Repository.

The value in this setting is not available for updates. If you must change the default value assigned to this setting, contact the Customer Services Support team.

**Database User ID (IBI\_REPOS\_DB\_USER)**

Specifies the user ID used by the JDBC driver to access the Repository.

The value in this setting is not available for updates. If you must change the default value assigned to this setting, contact the Customer Services Support team.

**Update Last Access Time (IBI\_UPDATE\_LAST\_ACCESS)**

Specifies whether the Last Accessed On property is updated in the Properties dialog box when a resource is accessed. The default value is ON, which indicates that the property is updated.

**Reference: Source Code Management Settings**

Source Code Management settings activate the use of a third-party source control provider with WebFOCUS or App Studio. They also identify the location of the server and root project where the source control provider repository is stored.

**Enable Source Control (IBI\_SCM\_ENABLE)**

When selected, this check box enables the integration of a source control provider to manage application code development in WebFOCUS or App Studio.

This check box and the Enable private working area (IBI\_SCM\_PWA\_ENABLE) check box must be selected to activate the use of Git Source Control operations within WebFOCUS.

**Provider (IBI\_SCM\_PROVIDER\_TYPE)**

Identifies the source control providers that are available for use when working with WebFOCUS or App Studio.

You can select the source control provider that you want to use from the list of available providers included in this setting.

☐ **Git.** Supports source control operations from WebFOCUS.

☐ **Team Foundation Server.** Supports source control operations from App Studio.

Typically, the applications created by these providers are installed on the same machine as the host server for WebFOCUS or App Studio.

**Version (IBI\_SCM\_PROVIDER\_VERSION)**

Identifies the version number of the source control provider that is specified in the Provider (IBI\_SCM\_PROVIDER\_TYPE) setting.

For example, when using Team Foundation Server 2013, type the value 2013.

This setting is not relevant to Git. Leave this setting blank when using Git as the source control provider.

**Enable private working area (IBI\_SCM\_PWA\_ENABLE)**

When selected, this check box enables the use of a private working area for source control operations within WebFOCUS or App Studio.

This check box and the Enable Source Control (IBI\_SCM\_ENABLE) check box must be selected to activate the use of Git Source Control operations within WebFOCUS.

### **Location of Source Code Configuration (IBI\_SCM\_REPOSITORY\_LOCATION)**

Identifies the URL of the server hosting the Team Foundation Server, including the collection name that is used to host the projects.

For example, when using Team Foundation Server 2013, type a value that uses the format `http://TFS_hostname:port/tfs/collection_name`.

This setting is not relevant to Git. Leave this setting blank when using Git as the source control provider.

### **Location of Root Project (IBI\_SCM\_ROOT\_PROJECT\_LOCATION)**

Identifies the path and folder name where the root source control project was installed.

For example, when using Team Foundation Server 2013, type the value `$/TeamProject1`.

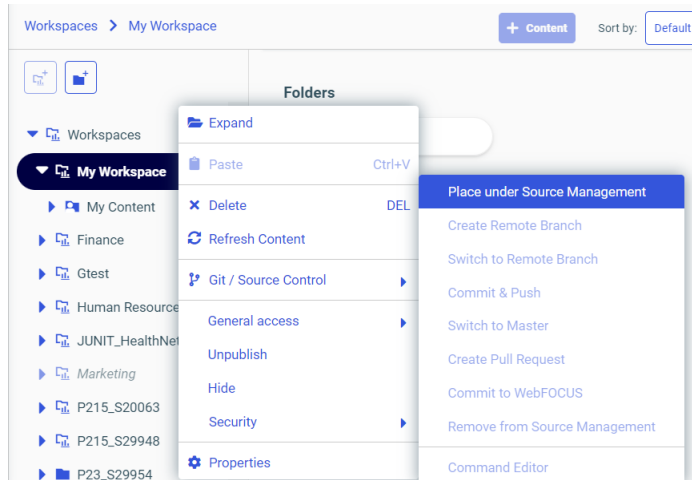
This setting is not relevant to Git. Leave this setting blank when using Git as the source control provider.

## ***Procedure:* How to Configure a Source Control Provider for the WebFOCUS Home Page**

Before you attempt to configure a source control provider, ensure that all providers that could be made available to WebFOCUS users in the Provider (IBI\_SCM\_PROVIDER\_TYPE) setting list have been configured and are housed in a network location that is available to WebFOCUS.

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, select *Source Code Management* to display the Source Code Management page.
3. Select the *Enable Source Control (IBI\_SCM\_ENABLE)* setting check box.
4. Select the *Enable private working area (IBI\_SCM\_PWA\_ENABLE)* setting check box.
5. Select *Git* from the Provider (IBI\_SCM\_PROVIDER\_TYPE) setting list.
6. Leave the remaining settings in the Source Control Management section blank, as shown in the following list.
  - ☐ Version (IBI\_SCM\_PROVIDER\_VERSION)
  - ☐ Location of Source Code Configuration (IBI\_SCM\_REPOSITORY\_LOCATION)
  - ☐ Location of Root Project (IBI\_SCM\_ROOT\_PROJECT\_LOCATION)
7. Click **Save**.
8. When you receive a message stating that your changes were saved successfully, click **OK**.

9. From the Administration Console Menu bar, click *Clear Cache*.
10. When you receive a message that the cache was cleared successfully, click *OK*.
11. Sign out of your current session.
12. Sign in again, and open the Workspaces view.
13. In the Resources tree or in the Content Area, right-click a Workspace and confirm that the Git/Source Control command appears on the shortcut menu as shown in the following image.



### **Procedure:** How to Configure a Source Control Provider for TIBCO WebFOCUS App Studio

Before you attempt to configure a source control provider, ensure that all providers that could be made available to App Studio users in the Provider (IBI\_SCM\_PROVIDER\_TYPE) setting list have been configured and are housed in a network location that is available to WebFOCUS.

1. Sign in as an administrator, and open the Administration Console.
2. On the Configuration tab, under the Application Settings folder, select *Source Code Management* to display the Source Code Management page.
3. Select the *Enable Source Control (IBI\_SCM\_ENABLE)* setting check box.
4. Select the application that will manage source control operations for WebFOCUS in the Provider (IBI\_SCM\_PROVIDER\_TYPE) setting list.

For example, Team Foundation Server.

5. Enter the version number of the source control provider you specified in the Provider field in the Version (IBI\_SCM\_PROVIDER\_VERSION) setting field.

For example, when using Team Foundation Server 2013, type the value 2013.

6. Enter the URL of the server hosting the source control provider, including the collection name that is used to host the projects, in the Location of Source Code Configuration (IBI\_SCM\_REPOSITORY\_LOCATION) setting field.  
  
For example, `http://TFS_hostname:port/tfs/collection_name`.
7. Enter the path and folder name where the root source control project was installed in the Location of Root Project (IBI\_SCM\_ROOT\_PROJECT\_LOCATION) setting field.  
  
For example, `$/TeamProject1`.
8. Click Save.
9. When you receive a message stating that your changes were saved successfully, click OK.
10. From the Administration Console Menu bar, click *Clear Cache*.
11. When you receive a message that the cache was cleared successfully, click OK.
12. Test your configuration.

### **Reference:** Search Settings

Search settings configure general Search operations. They apply to Solr Search.

#### **Solr Cloud (IBI\_INFOSEARCH\_SOLR\_CLOUD)**

This information is not yet available.

#### **Solr Connection Timeout (ms) (IBI\_INFOSEARCH\_SOLR\_TIMEOUT\_MILLISECONDS)**

This information is not yet available.

#### **Solr URL (IBI\_INFOSEARCH\_SOLR\_URL)**

Identifies the URL of the Solr server for your product installation. When Solr is the designated search engine, the WebFOCUS Client directs indexing and search queries to this URL.

When this value is blank, no URL is identified and no connection can be made to the Solr server engine from the WebFOCUS Client. This setting is blank, by default.

If you are using an IBCloud installation, the cloud administrator must provide you with the correct URL and port number to assign to this setting.

If you are using your own SolrCloud or Solr stand-alone installation, you must identify the URL of the Solr Server in use in your organization and assign it to this value.

For a single cluster Solr configuration, in a non-SolrCloud installation, the format of the Solr URL is:

`<scheme>://<host>:<port>/solr`

Where:

*scheme*

Is the scheme in use in your organization. We recommend https.

*host*

Is the name of the machine that hosts the WebFOCUS Reporting Server.

*port*

Is the number of the port you use to connect to the Solr search engine.

For example: https://host\_name:8983/solr

### **Maximum Number of Search Results (IBI\_MAGNIFY\_RECORDLIMIT)**

Specifies the maximum number of search results returned by a search request. Any results beyond this number are not displayed to the user. The default value is 300 results.

### **Collection Name (IBI\_SEARCH\_COLLECTION)**

This setting is relevant only if your organization uses the Basic Authentication plugin with the Apache Solr search engine.

If Solr Basic authentication is not in use, this setting is blank.

If Solr Basic authentication is in use, this setting contains the name of the collection that contains your search data and is accessible only with a valid Solr username and password. This value can be authenticated only if a collection name is also defined in the Solr Collections API. This is the default value.

The value *ibi-protected* appears in this setting, by default. If you do not use the default value, you must assign a unique name to this field, and assign the same unique name to your collection in the Solr Collections API.

For more information, see the *Collections/Core Admin* topic and the *Collections API* topic in the *Apache Solr Reference Guide*.

### **Password for Basic Authentication (IBI\_SEARCH\_PASSWORD)**

This setting is relevant only if your organization uses the Basic Authentication plugin with the Apache Solr search engine.

A password appears in this setting by default. It is assigned to this setting during product installation. If not in use, leave as is. If in use, replace default password with the password used by your Solr administrator.

If Solr Basic authentication is in use, this setting contains the password that authenticates Solr-based indexing and search queries. This value can be authenticated only if a password is assigned to the security.json file in the Basic Authentication plugin.

If you are working within an IB Cloud installation, you must assign the password provided to you by the Customer Support team to this field.

If you create your own Solr installation, you must create your own password, assign it to this field, and to the password field of the security.json file in the Basic Authentication plugin.

For more information see the *Basic Authentication Plugin* topics in the *Apache Solr Reference Guide*.

### **Username for Basic Authentication (IBI\_SEARCH\_USERNAME)**

This setting is relevant only if your organization uses the Basic Authentication plugin with the Apache Solr search engine.

If Solr Basic authentication is not in use, this setting is blank. This is the default value.

If Solr Basic authentication is in use, this setting contains the user name that authenticates Solr-based indexing and search queries. This value can be authenticated only if a user name is assigned to the security.json file in the Basic Authentication plugin.

If you are working within an IB Cloud installation, you must assign the user name provided to you by the Customer Support team to this field.

If you create your own Solr installation, you must create your own user name, assign it to this setting, and assign it to the username field of the security.json file in the Basic Authentication plugin.

For more information, see the *Basic Authentication Plugin* topics in the *Apache Solr Reference Guide*.

## **Configuring Solr Basic Authentication**

Solr Basic authentication supports the authentication of Solr-based indexing and search queries. It is managed by the Solr Basic authentication plugin, and is required when working in the multi-tenant IB Cloud product to help maintain discrete data for each tenant.

In order to authenticate a query or index operation when using Solr Basic authentication, the user name and password sent from WebFOCUS must match the user name and password as defined in the security.json file, and the collection name must match the name of the collection to which Solr searches are directed as defined in the name parameter of the Collections API. Therefore, these values must be established both in WebFOCUS and in the SolrCloud or Solr stand-alone server installation.



If you are working in IB Cloud or in another shared cloud environment, the administrators of that cloud environment will provide you with a username, password, and collection name for your search data. If you are creating your own Solr installation you must create your own username, password, and collection name and include them in its configuration.

When you have been provided with these values or created them for yourself, enter them in the Basic Authentication settings on the Search settings page of the Administration Console Configuration tab.

If you are creating your own Solr installation, you must also create a `security.json` file within the Apache Solr Basic authentication plugin and assign the user name and password to the username and password tags. You must also create a new collection in the Collections API and assign the collection name to it.

For information about how to assign a value to a setting in the Administration Console, see [How to View or Edit Application Settings](#) on page 123 of the *Security and Administration* technical content. For information about how to create a `security.json` file and the values it contains, see the *Enable Basic Authentication* topic in the *Apache Solr Reference Guide*. For information about how to create a collection and assign a collection name, see the *Collections/Core Admin* topic and the *Collections API* topic in the *Apache Solr Reference Guide*.

### **Reference: Text Generation Server Settings**

Text Generation Server settings define the connections to an independent server that provides narrative descriptions for chart headers, footers, and tooltips.

#### **Text Generation Server URL (IBI\_TEXT\_GENERATION\_SERVER\_URL)**

Identifies the URL of the external natural language generation (NLG) server that provides narrative descriptions for chart headers, footers and tooltips. If your product installation supports natural language generation for charts, type the URL of the text generation server in this setting. This setting is blank, by default.

When you activate the use of an external natural language generation (NLG) server, this setting contains a value, typically:

[http://machine\\_name:20000/yseop-manager/direct/savvy-kb/dialog.do](http://machine_name:20000/yseop-manager/direct/savvy-kb/dialog.do)

Where:

[machine\\_name](#)

Is the name of the server that hosts the external natural language generator.

**Reference: Validation Settings**

Validation settings specify the behavior of WebFOCUS when validation tests fail.

**Note:** The character patterns IBI, IBIFS, and PG\_ are reserved for internal product variables. They should not be used at the beginning of variable names.

**Validate (IBI\_VALIDATE\_ACTION)**

Specifies the action to take if a URI-parameter validation test fails. The validation test is performed as a precaution against SQL injection and cross-site scripting attacks. Permitted values are:

- ☐ **Log Only.** WebFOCUS allows the request but logs the validation failure in the *drive:\ibi\WebFOCUS82\logs\websecurity.log* file.
- ☐ **Custom Enforcement and Log. (ENFORCE)** WebFOCUS blocks the request, logs the failure in the *drive:\ibi\WebFOCUS82\logs\websecurity.log* file, and takes the action specified by IBI\_Validate.Error\_Response.
- ☐ **Default Enforcement and Log. (XMLENFORCE)** WebFOCUS blocks the request, logs the failure in the *drive:\ibi\WebFOCUS82\logs\websecurity.log* file, and returns a descriptive XML response with an HTTP status code of 200 (success). This is the default and recommended setting.

**Custom Response (IBI\_VALIDATE\_ERROR\_RESPONSE)**

Specifies the HTTP response code to return to the browser when URI-parameter validation has failed and IBI\_Validate.Action is set to ENFORCE. Permitted values are any valid HTTP status code (such as 400 or 403), a URI, or a fully qualified URL. If an HTTP status code is entered, WebFOCUS returns a response header with the status code. If a URL or URI is entered, WebFOCUS returns 200 (success) and redirects the browser to the specified address. The default value is 400.

**Response Header (IBI\_VALIDATE\_RESPONSE\_HEADER)**

For diagnostic purposes only. If True, returns an HTTP response header to the browser specifying the URLs that failed validation and the reason for their failure. The default value is False.

**TIBCO WebFOCUS Designer Properties**

Settings on the Designer Properties page of the Administration Console determine the display and use of features in WebFOCUS Designer. To open this page, in the Administration Console, scroll down to the bottom of the Configuration tab menu, and then select *Designer Properties*.

**Reference: Understanding WebFOCUS Designer Properties**

Administrators can use the settings on the Designer Properties page to specify default values assigned to WebFOCUS Designer settings.

If the *Allow User Override* check box is selected for an option, users can change the value assigned to the setting by the administrator.

**Data Preview Method**

Sets the default action for whether charts and reports are previewed by using sample data, actual live data from the data source, or dummy test data. Valid values for the Data Preview Method setting are *Sample*, *Live*, and *Test*. The default value is *Live*.

If the *Allow User Override* check box is selected for this option, users can change the value assigned to the setting by the administrator in WebFOCUS Designer.

**Record Limit**

Sets the default maximum number of rows retrieved from the data source when the design-time preview is created. This feature is useful in reducing response time if users are working with a large amount of data. The Record Limit setting does not affect the chart or report output at run time. Valid values for the Record Limit setting are *100*, *500*, *1000*, *5000*, *10000*, and *All* rows. The default value is *500* rows.

If the *Allow User Override* check box is selected for this option, users can change the value assigned to the setting by the administrator in WebFOCUS Designer.

This setting is unavailable if *Test* is selected as the Data Preview Method.

**Enforce Limit**

Sets the default action that determines whether the record limit must be applied to the data source before or after creating a design-time preview. This setting is used only if *Live* is selected as the Data Preview Method. Valid values for the Enforce Limit setting are *At the Source* and *Post Retrieval*. If *At the Source* is selected as the Enforce Limit value, then the record limit is applied to the data source before the design-time preview is generated. If *Post Retrieval* is selected as the Enforce Limit value, then the record limit is applied to the data source after the design-time preview is generated. The default value is *Post Retrieval*.

If the *Allow User Override* check box is selected for this option, users can change the value assigned to the setting by the administrator in WebFOCUS Designer.

**InfoAssist Properties**

Settings in the InfoAssist Properties page of the Administration Console determine the display and use of features in the InfoAssist tool that opens when creating or updating content.

To open the InfoAssist Properties page, in the Administration Console, scroll down to the bottom of the Configuration tab menu, and then click *InfoAssist Properties*. You can then enable or disable options for the InfoAssist tool.

### **Reference:** Understanding InfoAssist Home Tab Properties

VaThe InfoAssist Home tab enables you to control the most commonly used properties and options from the Home tab. These properties are:

#### **Use Live Preview Mode**

Determines whether InfoAssist opens in the Live Preview mode or the Query Design View, by default. When Yes is selected, InfoAssist opens in the Live Preview mode as the default. When Yes is not selected, InfoAssist starts with the Query Design View. If the *Allow User Override* check box is selected for this option, users can change the setting specified by the administrator.

#### **Record Limit**

Enables the Record Limit menu of the Home tab. If *Show* is not selected, the Record Limit menu is removed from the InfoAssist interface.

#### **Themes**

Provides InfoAssist users with various color-coded StyleSheet themes that can be used to style reports and charts. Users can select standard themes, or select customized cascading style sheet themes created by your organization.

#### **Page Heading**

Enables the Header & Footer menu of the Home tab. This menu can be used to add a heading or footing to each page of the report output.

#### **Report Heading**

Enables the Header & Footer menu of the Home tab. This menu can be used to add a heading or footing to the first page of the report output.

### **Reference:** Understanding InfoAssist Format Tab Properties

For reports or charts, InfoAssist displays a list of output file format options, such as HTML, PDF, or Excel, in the Format Group of the Home tab. Other options that make additional layouts and display features available when creating a report or chart appear on the Format tab itself. You can control the display of both types of options through the settings contained in this section.

**Note:** Settings in this section do not affect the display of Format tab features for visualizations.

### **PDF Analytic Document Format**

Enables the use of the PDF Analytic Document Format in InfoAssist. This format adds the portability and interactive enhancements of In-Document Analytics to PDF reports. The resulting output is designed for offline analysis and includes all of the data and JavaScript tools required to support analytic operations such as filtering, sorting, and charting in a self-contained report.

When this check box is selected, this format is available as an option in the Output File Format list that opens from the Format group of the InfoAssist Home Page ribbon. It is also available for selection as a default output format from the Report Output Format list, the Chart Output Format list, and the Document Output Format list in the Tool Options Dialog Defaults section of the InfoAssist Properties page.

This check box is cleared, by default.

### **HTML Analytic Document Format**

Enables the use of the HTML Analytic Document Format in InfoAssist. This format adds the portability and interactive enhancements of In-Document Analytics to HTML reports. The resulting output is designed for offline analysis and includes all of the data and JavaScript tools required to support analytic operations such as filtering, sorting, and charting in a self-contained report.

When this check box is selected, this format is available as an option in the Output File Format list that opens from the Format group of the InfoAssist Home Page ribbon. It is also available for selection as a default output format from the Report Output Format list, the Chart Output Format list, and the Document Output Format list in the Tool Options Dialog Defaults section of the InfoAssist Properties page.

This check box is selected, by default.

### **Additional HTML Formats for Chart**

Enables the use of the PNG, JPEG, GIF, and SVG output formats. The default value is PNG. PNG is not available as a format for chart output.

### **Additional PDF Formats for Chart**

Enables the use of the PDF/SVG and PDF/GIF output formats. The default value is PDF/SVG.

### **Excel 2000 Format**

Enables the use of the Excel 2000 spreadsheet output format. The Excel 2000 format supports most StyleSheet attributes, allowing for full report formatting. The computer on which the report displays must have Microsoft Excel 2000 installed.

When this check box is selected, this output format option is available for use when selected from the Output Format drop-down menus in the Tool Options Dialog Defaults section.

This check box is selected, by default.

### **Excel 2000 Formula**

Enables the use of the Excel 2000 formulas when the *Excel 2000 Format* option is selected.

This check box is selected, by default.

### **Excel 2007 Format**

Enables the use of the Excel 2007 spreadsheet output format. The computer on which the report displays must have Microsoft Excel 2007 installed.

When this check box is selected, this output format option is available for use when selected from the Output Format drop-down menus in the Tool Options Dialog Defaults section of the InfoAssist Properties page.

This check box is selected, by default.

### **Excel 2007 Formula**

Enables the use of the Excel 2007 formulas when the *Excel 2007 Format* check box is selected.

This check box is selected, by default.

### **Excel Pivot**

Enables the use of the Excel 2000 PivotTable output format. PivotTable is an Excel tool for analyzing complex data.

This check box is not selected, by default.

### **Excel CSV**

Enables the use of the comma separated values (CSV) file format.

When this check box is selected, the Excel CSV format option is available for use in InfoAssist, and it appears on the *Home* tab in the Format group options list under the Excel format option. When it is cleared, this option is not available, and it does not appear in the Format group options list.

This check box is selected, by default.

### **HTML Format**

Enables the use of the HTML page report format.

When this check box is selected, this output format option is available for use when selected from the Output Format drop-down menus in the Tool Options Dialog Defaults section of the InfoAssist Properties page.

### **InfoMini Run Immediate**

If *Enable* is selected, reports run immediately when InfoMini first launches. This setting is enabled, by default.

### **Other Chart Types**

Allows the creation of more complex graph output types, such as spectral maps, gauge charts, and Pareto charts.

### **Pages on Demand**

Enables the display of report output one page at a time. Users can use the navigation menu at the bottom of the output screen to view each page. This option is activated only when HTML or active report output format is selected.

### **PDF Format**

Enables the use of the PDF report format.

When this check box is selected, this output format option is available for use when selected from the Output Format drop-down menus in the Tool Options Dialog Defaults section of the InfoAssist Properties page.

### **PowerPoint 2000 Format**

Enables the use of the PowerPoint® 2000 document output format. The computer on which the report appears must have Microsoft PowerPoint 2000 or higher installed.

When this check box is selected, this output format option is available for use when selected from the Output Format drop-down menus in the Tool Options Dialog Defaults section of the InfoAssist Properties page.

### **PowerPoint 2007 Format**

Enables the use of the PowerPoint® 2007 document output format. The computer on which the report appears must have Microsoft PowerPoint 2007 or higher installed.

When this check box is selected, this output format option is available for use when selected from the Output Format drop-down menus in the Tool Options Dialog Defaults section of the InfoAssist Properties page.

### **Stack Measures**

Displays all numeric measure field names in the first column of the report output, with the corresponding numeric data values displayed across time in a column for each selected time period. The Stack Measures feature is activated only when HTML, Excel, or PowerPoint output format is selected.

### **User Selection**

Allows users to change the output type of their reports at run time.

### ***Reference:* Understanding InfoAssist View Tab Properties**

Enables InfoAssist users to customize the view of different report components in the InfoAssist tool, such as the design mode, output location, and data view. You can configure the following properties in the InfoAssist View tab:

#### **Display View Tab**

Enables the View tab and all of its menu options. If this is not selected, the View tab is removed from the InfoAssist interface.

#### **Data Panel**

Allows the user to customize Data Panel settings. Values are *Logical* (default), *List*, and *Structured*.

#### **Query Panel**

Allows the user to customize the view of the query components, such as Filters, Column and Row labels, and Measures when building a report. Values are *Tree* (default), *Area 2x2* (2 columns by 2 rows), *Area 1x4* (1 column by 4 rows). If the *Allow User Override* check box is selected for this option, users can change the setting specified by the administrator.



**Reference: Understanding InfoAssist Tool Options Dialog Defaults Properties**

Settings in the Tool Options Dialog Default section enable administrators to specify default tool settings. If the *Allow User Override* check box is selected for an option, users can change the setting specified by the administrator. However, the administrator cannot specify a default value that has already been disabled in one of the other groups. For example, if you have disabled the PDF Analytic Document Format option in the Format Tab section, you will receive an error message if you attempt to set that format as a default Report, Chart, or Document Output Format in the Tools Options Dialog Defaults section.

**Report Output Format**

Sets the default format for reports. Valid values are *HTML*, *HTML Analytic Document*, *PDF*, *PDF Analytic Document*, *EXL07*, *EXL2K*, *PowerPoint 2000*, and *PowerPoint 2007*. The format options in this list are available only when their corresponding check box is selected in the Format Tab section of the InfoAssist Properties page. If that check box is cleared, you receive a message warning you that the format option is not enabled when you select it from this list. The default value is *HTML*.

**Chart Output Format**

Sets the default format for charts. Valid values are *HTML*, *HTML5*, *HTML Analytic Document*, *PDF*, *PDF Analytic Document*, *EXL07*, *EXL2K*, *PowerPoint 2000*, and *PowerPoint 2007*. The format options in this list are available only when their corresponding check box is selected in the Format Tab section of the InfoAssist Properties page. If that check box is cleared, you will receive a message warning you that the format option is not enabled when you select it from this list. The default value is *HTML5*.

**Document Output Format**

Sets the default format for documents that are generated in InfoAssist. Valid values are *HTML*, *HTML Analytic Document*, *PDF*, *PDF Analytic Document*, *EXL07*, *EXL2K*, *PowerPoint 2000*, and *PowerPoint 2007*. The format options in this list are available only when their corresponding check box is selected in the Format Tab section of the InfoAssist Properties page. If that check box is cleared, you will receive a message warning you that the format option is not enabled when you select it from this list. The default value is *HTML Analytic Document*.

**Page Orientation**

Sets the default page orientation for reports and charts. Valid values are *Portrait* and *Landscape*. The default value is *Landscape*. If the *Allow User Override* check box is selected for this option, users can change the setting specified by the administrator.

### **Page Size**

Sets the default page size for reports and charts. Valid values are *A3*, *A4*, *A5*, *Letter*, *Tabloid*, *Legal*, *PPT-SLIDE*, and *Large Size*. The default value is *Letter*. If the *Allow User Override* check box is selected for this option, users can change the setting specified by the administrator.

### **Data Preview Method**

Sets the default action for whether reports are previewed using sample data or actual data from the data source. Valid values are *Live* and *Sample*. The default value is *Live*. If the *Allow User Override* check box is selected for this option, users can change the setting specified by the administrator.

### **Record Limit**

Sets the default maximum number of rows retrieved from the data source when Interactive Design view is selected. This feature is useful in reducing response time if users are working with a large amount of data. It is applicable only when developing the report. The record limit setting will not affect the report output at run time. Valid values are, *All*, *1*, *10*, *50*, *100*, *500*, *1000*, *2000*, *5000*, *10000* rows. The default value is *500* rows. If the *Allow User Override* check box is selected for this option, users can change the setting specified by the administrator.

### **Output Target**

Sets the default location for reports and charts. Valid values are *Single tab*, *New tab*, *Single window*, and *New window*. The default value is *Single tab*. If the *Allow User Override* check box is selected for this option, users can change the setting specified by the administrator.

### **In-Document Analytics**

Sets the default value for the In-Document Analytics setting in the Procedure Settings dialog box, which opens from the InfoAssist Quick Access toolbar. Valid values are *Designer Style* and *Legacy*. In the InfoAssist Properties page setting, the *Designer Style* value is selected, by default.

The value assigned to this setting determines the default interface for InfoAssist to use when running reports, charts, and documents based on the HTML Analytic Document format. When users create new HTML Analytic reports, charts, and documents in InfoAssist, they can override the default value established in the InfoAssist Properties page setting by selecting an alternative option from the In-Document Analytics setting that appears in the Procedure Settings dialog box.

**InfoAssist/Portal StyleSheet**

Sets the StyleSheet to be used for InfoAssist and the Portal. Click *Change Stylesheet* to open the Browse predefined template files window. The value displayed, by default, is *Warm.sty*.

If the *Allow User Override* check box is selected for this option, users can change the setting specified by the administrator.

**Visualization StyleSheet**

Sets the StyleSheet to be used when creating visualizations. Click *Change Stylesheet* to open the Browse predefined template files window. The value displayed, by default, is *Warm.sty*.

If the *Allow User Override* check box is selected for this option, users can change the setting specified by the administrator.

**Encode HTML**

Encodes script tags within data, so that the tags are replaced and not executable in a browser. The default value is Yes. This includes the ON TABLE SET HTMLENCODE ON command in the procedure.

**Enable Pages On Demand**

Allows InfoAssist users to view report output one page at a time. The user can use the navigation menu at the bottom of the output screen to view each page. This option is activated only when HTML or active report output format is selected.

**Rows retrieved from cache**

Establishes how many rows of cached data stored in a binary file are returned to the output window at one time. The default value is 100 rows.

**HTML Freeze Height**

Determines how the Freeze option, located on the *Format* tab in the *Navigation* group of the InfoAssist ribbon, automatically freezes the height of a report area.

If the AutoFit value is assigned to this setting, reports produced when the Freeze option is selected automatically fit the height of the window or pane in which they appear. This is the default value.

If the Fixed value is assigned to this setting, reports produced when the Freeze option is selected are set automatically to a fixed height of four inches, regardless of the size of the window or pane in which they appear.

### HTML Accordion

Determines whether the Accordion option, located on the *Format* tab in the *Navigation* group of the InfoAssist ribbon, displays accordion reports that automatically resize data to fit the container in which they appear.

If the AutoFit value is assigned to this setting, reports produced when the Accordion option is selected automatically resize the display of data to fit the size of the container in which they appear, and automatically adjust column widths based on the size of the largest data value or column title. This is the default value.

If the legacy value is assigned to this setting, reports produced when the Accordion option is selected do not automatically resize the display of data to fit the size of the container in which they appear, and do not automatically adjust column widths.

## Enabling the Cache Through Global Preferences

In InfoAssist, the cache option enables you to send only the first page of report output using the Analytic Document Format to the browser and retrieve subsequent pages from a temporary cache on the WebFOCUS Reporting Server. You can enable the cache locally through the Advanced tab of the Analytic Document Options dialog box in InfoAssist. You can enable the cache option globally by configuring the relevant InfoAssist Properties settings in the WebFOCUS Administration Console. For more information about the impact of these settings on InfoAssist, see the *Using the Cache Option* section of the *TIBCO WebFOCUS® InfoAssist User's Manual*.

### **Procedure:** How to Enable the Cache Through InfoAssist Properties

You can globally enable the cache for InfoAssist by using settings in the Administration Console, as described in the following steps:

1. Open the Administration Console.
2. On the Configuration tab, click *InfoAssist Properties*.
3. On the InfoAssist Properties page, under the Tool Options Dialog Defaults section:
  - a. Select the Yes checkbox, in the Enable Pages On Demand setting.
  - b. Accept the default value of 100 in the Rows retrieved from cache setting, or type an alternative value that conforms to your requirements.
4. At the bottom of the page, click Save.
5. When you receive a message that the changes were saved successfully, click OK.

**Procedure: How to Validate the Cache Configuration**

You can confirm that InfoAssist uses the global settings you configure in the Administration Console, as described in the following steps:

1. Open InfoAssist to create a new report or edit an existing report.
2. On the *Home* tab, in the *Format* group, click the *Output File Format* list, and then click *HTML Analytic Document* or *PDF Analytic Document*.
3. Click the *Format* tab.
4. In the *Navigation* group, confirm that the *Pages on Demand* option is highlighted.
5. In the *Features* group, click *Analytic Document Options*.
6. In the *Analytic Document Options* dialog box, click *Advanced*.
7. Compare the value in the *Rows Retrieved* field to the value you accepted or typed in the *Rows retrieved from cache* setting in the Administration Console.

If the two values are a match, the Administration Console configuration update was a success. If they do not match, review your configuration of the Administration Console setting.

**Reference: Understanding InfoAssist File Options**

Determines which of the following file types can be selected by InfoAssist users when creating and saving HOLD files:

**Binary**

Stores report or chart data as binary numbers in numeric fields. Binary files use the extension (\*.ftm).

**FOCUS**

Stores report or chart data as text in a segment structure that conforms to FOCUS database requirements. FOCUS files use the extension (\*.foc).

**Comma Delimited with Titles**

Stores report or chart data as text in sequence by field. Alphanumeric fields are enclosed in quotation marks. Fields are separated by commas and are preceded by Field Names. Comma Delimited with Titles files use the extension (\*.csv) (Comma Separated Values).

**Plain Text**

Stores report or chart data as text in sequence by field without delimiters or field names. Plain Text files use the extension (\*.ftm).

### **Tab Delimited**

Stores report or chart data as text in sequence by field. Fields are separated by tab characters. Tab Delimited files use the extension (\*.tab).

### **Tab Delimited with Titles**

Stores report or chart data as text in sequence by field. Fields are separated by tab characters, and are preceded with field names. Tab Delimited with Titles files use the extension (\*.tab).

### **Database Table**

Stores report or chart data as text in a field structure that conforms to a Structured Query Language (SQL) Database format. Database Table files use the extension (\*.sql).

Database Table output is only available when working against an SQL database.

### **Hyperstage**

Stores report or chart data as text in a field structure that conforms to the Hyperstage database table format. Hyperstage files use the extension (\*.bht).

Hyperstage output is only available when the WebFOCUS Reporting Server has a Hyperstage adapter configuration.

### **SQL script**

Stores report or chart data as text in a sequential field structure that can be imported into a database table that conforms to the Structured Query Language (SQL) Database format. SQL Script files use the extension (\*.sql).

SQL Script output is only available when working against an SQL database.

### **XML**

Stores report or chart data as text in a field structure that conforms to the rules of the Extensible Markup Language. Fields are separated by tags that identify content. XML files use the extension (\*.xml).

### **JSON**

Stores report or chart data as text in a structure that conforms to the rules of JavaScript Object Notations. JSON files use the extension (\*.json).

**Reference: Understanding InfoAssist Chart Type Options****Leaflet Maps**

Enables the icons required for the use of Leaflet maps in both chart and visualization mode of InfoAssist. The two Leaflet map icons enable you to select either a Choropleth or a Proportional Symbol (Bubble) map based on the Leaflet open-source JavaScript library for mobile-friendly interactive maps.

In chart mode, these icons are available in the Select a chart dialog box. To open this dialog box, click *Other* on the Format tab, in the Chart Types group. In the Select a chart dialog box, click *Map*.

In visualization mode, these icons are available in the Select a Visual dialog box. To open this dialog box, click *Change* on the Home tab, in the Visual group.

If this setting is not selected, Leaflet map icons do not appear in either location. The default value is selected.

**Reference: Understanding InfoAssist Auto Drill Properties**

Settings in this section enable the use of drill-down navigation options, which are part of the Auto Drill functionality.

**Single Click Navigate**

Enables the use of single click navigation, which is an automatic drill down to the next level of a dimension within the body of a report or chart made in response to a single click on a top-level entry or feature.

By default, this check box is not selected, meaning that single click navigation is disabled, and top-level Auto Drill entries or features display the Drilldown menu in response to a single click. If this check box is selected, single click navigation is enabled, and instead of displaying the Drilldown menu, top-level Auto Drill entries or features automatically refresh the report or chart with results based on the next lower level of your selected dimension in response to a single click.

**Breadcrumbs**

Enables the display of a breadcrumb trail at the top of an Auto Drill report or chart.

By default, this check box is selected, and Auto Drill reports and charts display a breadcrumb trail. If this check box is cleared, Auto Drill reports and charts do not display a breadcrumb trail.

In an Auto Drill report or chart, a breadcrumb trail displays a series of links to previous versions that were generated as you drilled through each level of your selected dimension to reach the version currently on display.

### **Restore Original**

Enables the display of the Restore Original option in the Drilldown menu.

By default, this check box is selected, and the Restore Original option appears in the Drilldown menu. If this check box is cleared, the Restore Original option does not appear in the Drilldown menu.

In an Auto Drill report or chart, the Restore Original option returns you directly to the original version.

### **Drill Up**

Enables the display of the Drill up option in the Drilldown menu.

By default, this check box is selected, and the Drill up option appears in the Drilldown menu. If this check box is cleared, the Drill up option does not appear in the Drilldown menu.

In an Auto Drill report or chart, the selection of the Drill up option refreshes the display with results based on the next level above the current level of your selected dimension.

### **Drill Down**

Enables the display of the Drill down option in the Drilldown menu.

By default, this check box is selected, and the Drill down option appears in the Drilldown menu. If this check box is cleared, the Drill down option does not appear in the Drilldown menu.

In an Auto Drill report or chart, the selection of the Drill down option refreshes the display with results based on the next level below the current level of your selected dimension.

**Note:** In addition to disabling the Drill down option, clearing this setting also removes hyperlinks from top level report entries and the breadcrumb trail display from reports and charts. If the Single Click Navigate setting is also cleared, clearing the Drill Down setting effectively disables Auto Drill navigation tools in reports and charts that contain only the top level of a dimension value in their design. If the Single Click Navigate setting is selected, and the report or chart contains entries below the top level, clearing the Drill Down setting shifts the Single Click Navigation feature to those lower-level entries. However, because this setting also suppresses the display of the Drilldown menu, users will neither be able to restore the original version of the report or chart, nor will they be able to drill back up to a higher level.



**Reference: Understanding InfoAssist Miscellaneous Options****Use two-part file name**

If selected, this option requires the use of two-part file names, which specify the path to the Master File location. If not selected, a one-part file name must be used instead. The default value is selected.

**Expand Data Source Tree**

Determines whether the initial view of the data source tree is expanded or collapsed. If selected, the tree is expanded. If not selected, the tree is collapsed. The default value is selected.

**Join Tool**

Displays the Join menu option on the InfoAssist Data tab. If not selected, the Join menu option is removed from the Data tab. The default value is selected.


**Layout Tab**

Enables the Layout tab in the InfoAssist ribbon. If not selected, the Layout tab is removed from the InfoAssist ribbon. The default value is selected.

**Series Tab**

Enables the Series tab in the InfoAssist ribbon. The Series tab displays when working with charts and visualizations. It provides access to charting properties and options in the Properties, Line, and Pie menus. If not selected, the Series tab is removed from the InfoAssist ribbon. The default value is selected.

**Enable Path Enforcement**

Establishes the default condition of the Enforce Paths container  that appears at the top of the Data pane of the Resources panel in the InfoAssist Application Window.

When you move a field from the Data pane into a field container on the Query pane, path enforcement automatically limits the display of available fields in the Data Source Tree to those with valid logical connections, based on their multi-path relationships, to the field that moved into the field container.

When this check box is cleared, the default value for this setting, the Enforce Paths container is not enabled, by default. Under this condition, the display of available fields in the Data Source Tree does not change when users move a field into a field container in the Query pane. Within the InfoAssist session, users can click the Enforce Paths container to enable path enforcement.

When this check box is selected, the Enforce Paths container is enabled, by default. Under this condition, fields in the Data Source Tree with no logical connection to a field moved into a field container in the Query pane are dimmed and unavailable. Within the InfoAssist session, users can click the Enforce Paths container to disable path enforcement.

**Note:** When you save a new procedure, the current condition of the Enforce Paths container is saved with the procedure. When you re-open the procedure in the InfoAssist Application Window, the condition of the Enforce Paths container is established by the value stored in the procedure instead of the value assigned to the Enable Path Enforcement setting.

### InfoAssist Basic Properties

When your installation is only licensed for InfoAssist Basic, the InfoAssist Properties are limited to the following settings:

#### Format Tab

- ☐ *Additional HTML Formats for Chart*
- ☐ *Additional PDF Formats for Chart*
- ☐ *Excel 2000 Format*
- ☐ *Excel 2000 Formula*
- ☐ *Excel 2007 Format*
- ☐ *Excel 2007 Formula*
- ☐ *Excel Pivot*

#### Auto Drill

- ☐ *Single Click Navigate*
- ☐ *Breadcrumbs*
- ☐ *Restore Original*
- ☐ *Drill Up*
- ☐ *Drill Down*

#### Miscellaneous

- ☐ *Use two-part file name*

## Logging

---

This topic explains how to access and interpret the audit logs of security events.

**In this appendix:**

- ☐ [Daily Log and Trace File Maintenance](#)
  - ☐ [Understanding Audit Logs](#)
  - ☐ [Understanding Monitor Logs](#)
  - ☐ [Understanding the Monitor ID](#)
  - ☐ [Understanding Change Management Import and Export Logs](#)
  - ☐ [Understanding the Advanced Web Tools, BI Portal, Event, EclipseLink JPA, and ReportCaster Log](#)
- 

### Daily Log and Trace File Maintenance

Log and trace files can accumulate a great deal of data in a short time. As these files grow, they require more storage and operational resources, and more time to complete searches and investigations. Therefore, most clients retain log and trace files only for a limited period.

To minimize this backlog, log files or trace files are removed automatically after the period defined in the settings, *Days Until Logs Are Deleted* (*IBI\_LOG\_RETAIN\_DAYS*), and *Days Until Traces Are Deleted* (*IBI\_TRACE\_RETAIN\_DAYS*). The default storage period for both settings is ten days, but you can assign any number between 1 and 3650 to lengthen or shorten the storage period. You can find these settings on the Application Directories page, of the Configuration tab, in the Administration Console.

To measure the storage period for an individual log file or trace file, a time stamp is assigned to it that identifies when the last posting to the file occurred.

Each day at midnight, the date in the time stamp is automatically compared to the current date. If the difference between those dates exceeds the number of days identified in the settings, the newly outdated log file is deleted automatically.

For example, if the value assigned to the *Days Until Logs Are Deleted* (*IBI\_LOG\_RETAIN\_DAYS*) setting is ten days, the audit.log file that was created ten days prior is deleted automatically. This automated review may take place as early as a minute before midnight or as late as a minute after midnight.

Even though daily log and trace file maintenance settings automatically prevent the accumulation of an unmanageable backlog of log files and trace files, they also prevent files that contain records of problems or unexpected events from being permanently saved. To ensure that any log file or trace file remains available for analysis as long as necessary, you may need to create duplicate copies and store them in a secure location.

Understanding  
Audit Logs

Audit logs capture records of system administration activities, including records of system configuration events, changes to roles, rules, and content ownership, user administration activities, and sign-in and sign-out events. For security purposes, audit logs are always enabled.

The audit log file is located in the *drive:\ibi\WebFOCUS82\logs* directory, and all events captured by the loggers assigned to it are logged to this single file.

The list of loggers that contribute records of events to the audit file appears next to the audit log name entry at the top of the Log Files page of the Administration Console Diagnostics tab, as shown in the following image. Specialized loggers that contribute events to this log, such as *com.ibi.uoa.roles*, capture routine events at the INFO level. The main logger *com.ibi.uoa* captures other non-specialized events at the ERROR level.

Log Files

Zip All

Reset All to default

Log Name	Logger Name	Log Level
audit	com.ibi.uoa	ERROR
	com.ibi.uoa.caster_config	INFO
	com.ibi.uoa.config	INFO
	com.ibi.uoa.content	INFO
	com.ibi.uoa.groups	INFO
	com.ibi.uoa.magnify	INFO
	com.ibi.uoa.ownership	INFO
	com.ibi.uoa.roles	INFO
	com.ibi.uoa.rules	INFO
	com.ibi.uoa.seats	INFO
	com.ibi.uoa.shares	INFO
	com.ibi.uoa.signin	INFO
	com.ibi.uoa.users	INFO

The log4j2.xml file, which is located at *drive:\ibi\WebFOCUS\_WFI\WebFOCUS\webapps\webfocus\WEB-INF\classes*, contains the default configuration of loggers and appenders that define the format and scope of log records captured for each log. The display of log names and loggers on the Log File page is based on the configuration in this file.

Audit logs remain available for the number of days defined in the *Days Until Logs Are Deleted (IBI\_LOG\_RETAIN\_DAYS)* setting on the Application Directories page of the Administration Console Configuration tab. By default, audit logs are saved for ten days. You can customize the amount of time that logs are saved by changing the number of days defined in this setting. Keep in mind, however, that any changes you make to this setting will affect the number of days that all logs, not just the Audit log, remain available.

### **Procedure: How to Access the Audit Log**

To view the audit log, you must sign in as an administrative user with access to the Administration Console.

1. In the Administration Console, click the *Diagnostics* tab.
2. Under the Diagnostics folder, click *Log Files*.
3. On the Log Files page, in the Log Name column, click the *audit* link.

The *audit.log* page opens.

Entries are listed in order of the time of their occurrence, earliest to most recent.

- ☐ Scroll down to review log event entries that occurred later in the day.
  - ☐ Click *Bottom* to go directly to the most recent entry.
  - ☐ Click *New trace lines* to display entries of system log events that occurred after you opened the log file for review.
4. To review the audit log from a previous day, click it in the drop-down list of recent audit log files at the top of the page.

Older logs appear with the date appended to their file name in the form *audit.log\_YYYY\_MM\_DD.log*. By default, logs are kept for ten days. This duration is determined by the value assigned to the Days Until Logs Are Deleted (*IBI\_Log\_Retain\_Days*) setting located on the Application Directories page of the Configuration tab.

## Customizing the Audit Log Configuration

The default configuration of log files defined in the log4j2.xml file is designed to support most product installations. Administrators can change this configuration to redirect events captured by one or more of the audit file loggers to a separate log file or database table not defined in the default configuration to conform to the requirements of their organization.

For example, you might want to redirect sign-in events and user security events to a separate database table, by capturing the following information:

- ☐ Sign-in attempts and sign-out attempts.
- ☐ User creation, modification, and deletion.
- ☐ User assignments to or removals from groups.

Note that any changes made to the log4j2.xml file itself will clear the configuration of log file names and their associated loggers displayed on the Log File page in the Administration Console. Therefore, we strongly recommend that you make a backup copy of the log4j2.xml file before you make any changes to the file so that you can restore this display when necessary. For more information, see [How to Create a Copy of the log4j2.xml File](#) on page 595.

Once you establish this backup copy, you can redirect records of sign-in events to a separate log file by adding a dedicated appender and logger to a copy of the log 4j2.xml configuration file. For more information, see [How to Redirect Audit Log Events to a Separate Log File](#) on page 596.

If you want to redirect records to a database table, you must create a dedicated table to capture them within the targeted database along with the addition of a dedicated appender and logger to the copy of the log4j2.xml file. For more information, see [How to Redirect Audit Log Events to a Separate Database Table](#) on page 597.

As an alternative to the display of loggers on the Log Files page, you can develop database reports to replace the display and connect directly to the log files stored in the `drive:\ibi\WebFOCUS_WFI\WebFOCUS\logs` directory, as shown in the following image.

The screenshot shows the 'Log Files' page in the WebFOCUS interface. On the left, a sidebar lists 'Log Files' under 'Diagnostics'. The main area displays a table of loggers with columns: Log Name, Logger Name, and Log Level. A callout box labeled 'Log Files without audit logs (com.ibi.uaa...)' points to the 'com.ibi.uaa' logger. Below this, another table shows a list of log files. A red circle highlights a specific log file, and a callout box points to it, stating 'replaced with WF Report produced from DBMS tables depicting UOA log entries'.

LOGGER	logName	LOGID	EVENTDATE	MESSAGE
com.ibi.uaa.content	04/29/21	user1	2021/04/29 13:56:14.000000	createFolder SUCCESS user:admin1 folder:IBFS\WFORepository\Getting_Started-ad
			2021/04/29 13:56:22.363000	createItem SUCCESS user:admin1 item:IBFS\WFOUserinfo\admin1\tracking.xml
			2021/04/29 13:56:22.363000	putItem SUCCESS user:admin1 item:IBFS\WFOUserinfo\admin1\tracking.xml
com.ibi.uaa.groups	04/29/21	user1	2021/04/29 13:56:14.014000	addUserToGroup SUCCESS user:reporter2703047681 group:IBFS\SSYS\GROUPS\Biv_L
com.ibi.uaa.ownership	04/29/21	admin1	2021/04/29 13:56:28.381000	makePrivate SUCCESS inherited:FALSE onPath:IBFS\WFORepository\Getting_Started--
com.ibi.uaa.seats	04/29/21	user1	2021/04/29 13:56:28.381000	UserSeatAssigned SUCCESS user:reporter2703047681 PortalUsers\PU group:uf_relatiBa
com.ibi.uaa.signin	04/29/21	user1	2021/04/29 13:56:54.273000	System Startup
		unknown	2021/04/29 12:40:28.737000	authentication Failure-unregistered_user User:safesoft\dfid\IAddr:127.0.0.1
			2021/04/29 13:56:53.220000	authentication Failure-BadPassword User:admin Status:ACTIVE (sAddr:0.0.0.0.0.0.1)
			2021/04/29 13:54:17.120000	authentication Failure-BadPassword User:admin Status:ACTIVE (sAddr:127.0.0.1)
			2021/04/29 13:55:58.723000	authentication Failure-BadPassword User:admin Status:ACTIVE (sAddr:127.0.0.1)
		user1	2021/04/29 13:56:28.393000	signin SUCCESS user:reporter2703047681 (sAddr:127.0.0.1 user:Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0)
		admin1	2021/04/29 13:55:15.707000	signin SUCCESS user:admin1 monitorid:581620e416223d (sAddr:0.0.0.0.0.0.1) user:Safari/537.36 Edg/90.0.818.48 userDescription:admin123456789
			2021/04/29 13:56:22.403000	signOut SUCCESS user:admin1 monitorid:581620e416223d
com.ibi.uaa.users	04/29/21	user1	2021/04/29 13:56:28.320000	createUser SUCCESS user:reporter2703047681 status:ACTIVE e-mail:descDeveloper
			2021/04/29 13:56:28.363000	putUser SUCCESS user:reporter2703047681 Property:PU

### Procedure: How to Create a Copy of the log4j2.xml File

If you must make changes to the log file configuration, we recommend that you first create a backup copy of the `log4j2.xml` file as described in this procedure.

1. In your file system, navigate to `drive:\ibi\WebFOCUS\webapps\webfocus\WEB-INF\classes`.
2. Copy the `log4j2.xml` file and paste it into the same directory.

#### Notes:

- ❑ Be careful to preserve the `xml` extension on the new copy.
  - ❑ During product installation, the `log4j2.xml.backup` file is also added to this directory as a failsafe. Do not alter or delete this file.
3. Assign a new name to the copy of the `log4j2.xml` file.

### Procedure: How to Identify the Audit Log Events to Include in a Separate Log File

Review the loggers identified in the table that appears in the topic, [Understanding Security Events](#) on page 603, and identify those loggers that capture the log messages you want to divert to a separate file.

For example, the *com.ibi.uoa.signin* logger captures records of sign-in, sign-out, and session expiration events. This is the logger you need to update if you wish to save sign-in events in a separate log file or database table.

**Note:** If you want to direct events from multiple loggers to the same file, include them in your selection. For example, to divert log records of sign-in and user maintenance events in the same file, you need to include the *com.ibi.uoa.signin* logger and the *com.ibi.uoa.users* logger.

### **Procedure:** How to Redirect Audit Log Events to a Separate Log File

1. Navigate to *drive:/ibi/WebFOCUS82/webapps/webfocus/WEB-INF/classes/*.
2. Open the *log4j2.xml* file, and go to the `<RollingFile name="LOGGua">` block in the `<Appenders>` section.
3. Beneath the closing tag for the LOGGua block, insert a new RollingFile appender, based on the following code sample, that saves the audit log events you wish to divert to a separate file identified in the appender.

```
<RollingFile name="appendername">
  <FileName>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/logfilename.log</FileName>
  <FilePattern>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/messagepattern-%d{yyyy-MM-dd}-%i.log</FilePattern>
  <PatternLayout>
    <Pattern>[%d] %-5p %-16.16c{1} %-16.16X{monitorID} %X{userId} %m
    %n</Pattern>
  </PatternLayout>
  <Policies>
    <TimeBasedTriggeringPolicy />
    <SizeBasedTriggeringPolicy size="20 MB" />
  </Policies>
</RollingFile>
```

Where:

*appendername*

Is the name of the new appender. Use a name that identifies the types of log messages diverted to the new file. For example, *signinout.log* for messages captured by the sign-in logger.

*logfilename*

Is the name of the new log file containing the diverted log messages.

*messagepattern*

Is the pattern of log messages captured by the logger that is using this appender.

In the following code example, events captured by the *com.ibi.uoa.signin* logger are redirected to a separate log file named *signinout.log*.



```

<RollingFile name="LOGUoaSignInOut">
  <FileName>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/signinout.log</FileName>
  <FilePattern>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/signinout-%d{yyyy-MM-dd}-%i.log</FilePattern>
  <PatternLayout>
    <Pattern>[%d] %-5p %-16.16c{1} %-16.16X{monitorID} %X{userId} %m
  %n</Pattern>
  </PatternLayout>
  <Policies>
    <TimeBasedTriggeringPolicy />
    <SizeBasedTriggeringPolicy size="20 MB" />
  </Policies>
</RollingFile>

```

4. Search for the name of each logger that captures the log messages you wish to redirect.
5. Replace the value in the ref attribute of the AppenderRef tag with the name of the new appender to identify the new appender block you created for them as the target of the appender reference, as shown in the following example.

```

<logger name="logger" level value="info" additivity="false">
  <AppenderRef ref="appender" />
</logger>

```

Where:

*logger*

Is the name of the logger that captures messages typically assigned to the audit log. For example, com.ibi.uoa.signin.

*appender*

Is the name of the new appender that will redirect messages from the selected logger to the new log file.

In the following example the *name="com.ibi.uoa.signin"* logger identifies the new *LOGUoaSignInOut* appender block as the target of the appender reference.

```

<logger name="com.ibi.uoa.signin" level value="info" additivity="false">
  <AppenderRef ref="LOGUoaSignInOut" />
</logger>

```

6. Save the file.

Log events are now recorded in the log file you identify in the new appender. For example, sign-in events are now recorded in the signinout.log file, which will appear in the All Clients list of traces.

### **Procedure: How to Redirect Audit Log Events to a Separate Database Table**

1. Create the database table that will be used to store the audit log information. The table must contain appropriate columns for the information captured by the log.

For example, you can create a table that captures the user IDs, date and time stamps, logger names, and audit events for sign-in, sign-out, and session termination events, with the following code prepared for a PostgreSQL © database.

```
CREATE TABLE public.wf_log
(
    eventdate timestamp with time zone,
    logger character varying(128) COLLATE pg_catalog."default",
    level character varying(12) COLLATE pg_catalog."default",
    logid character varying(128) COLLATE pg_catalog."default",
    message character varying(255) COLLATE pg_catalog."default",
    exception text COLLATE pg_catalog."default"

GRANT UPDATE, INSERT, SELECT ON TABLE public.wf_log TO webfocus;
```

2. Navigate to *drive:/ibi/WebFOCUS82/webapps/webfocus/WEB-INF/classes/*.
3. Open the log4j2.xml file, and go to the <RollingFile name="LOGuoa"> block in the <Appenders> section.
4. Add the JDBC Appender to the log4j2.xml file using one of the following code snippets.
  - a. If you want to transfer control of the connection to the external database, include a description of the ConnectionFactory class, as shown in the second line of the following example.

```
<JDBC name="LOGevent" tableName="public.wf_log">
  <ConnectionFactory
    class="com.ibi.log4j2.ConnectionFactory"
    method="getConnection" />
  <Column name="eventdate" isEventTimestamp="true" />
  <Column name="logger" pattern="%logger" isUnicode="false" />
  <Column name="level" pattern="%level" isUnicode="false" />
  <Column name="logid" pattern="%X{userId}" isUnicode="false" />
  <Column name="message" pattern="%message" isUnicode="false" />
  <Column name="exception" pattern="%ex{full}" isUnicode="false" />
</JDBC>
```

Where:

*LOGevent*

Is the name of the JDBC appender that redirects events captured by this logger to the external database table. For example, *LOGuoa*.

*logger*

Is the name of the existing logger that captures messages typically assigned to the audit log. For example, *com.ibi.uoa.signin*.

- b. If you want to retain control of the connection within WebFOCUS, include a DriverManager tag, as shown in the second line of the following example.

```

<JDBC name="LOGevent" tableName="public.wf_log">
  <DriverManager
    connectionString="jdbc:postgresql://localhost:5432/WebFOCUS82"
    driverClassName="org.postgresql.Driver"
    username="webfocus"
    password="webfocus" />
  <Column name="eventdate" isEventTimestamp="true" />
  <Column name="logger" pattern="%logger" isUnicode="false" />
  <Column name="level" pattern="%level" isUnicode="false" />
  <Column name="logid" pattern="%X{userId}" isUnicode="false" />
  <Column name="message" pattern="%message" isUnicode="false" />
  <Column name="exception" pattern="%ex{full}" isUnicode="false" />
</JDBC>

```

Where:

*LOGevent*

Is the name of the JDBC appender that redirects events captured by this logger to the external database table. For example, *LOGuaa*.

*logger*

Is the name of the existing logger that captures messages typically assigned to the audit log. For example, *com.ibi.uoa.signin*.

5. Determine where the information is logged and add an appender reference to the name of each existing logger you wish to include.

- ❑ To log information solely in the external database, use the following code:

```

<Logger name="logger" level="info" additivity="false">
  <AppenderRef ref="LOGevent"/>
</Logger>

```

Where:

*logger*

Is the name of the existing logger that captures messages typically assigned to the audit log. For example, *com.ibi.uoa.signin*.

*LOGevent*

Is the name of the JDBC appender that redirects events captured by this logger to the external database table. For example, *LOGuaa*.

- ❑ To log information both in WebFOCUS and in the external database, use the following code:

```

<Logger name="logger" level="info" additivity="false">
  <AppenderRef ref="LOGevent"/>
  <AppenderRef ref="LOGdb"/>
</Logger>

```

Where:

*logger*

Is the name of the existing logger that captures messages typically assigned to the audit log. For example, *com.ibi.uoa.signin*.

*LOGevent*

Is the name of the JDBC appender that redirects events captured by this logger to the external database table. For example, *LOGuoa*.

*LOGdb*

Is the name of the JDBC appender that redirects events captured by this logger to the external database table.

6. If the *drive:/ibi/WebFOCUS82/webapps/webfocus/webfocus.war* file is deployed on the Application server, update and redeploy the webfocus.war file.
7. If the *drive:/ibi/ WebFOCUS82/webapps/webfocus* expanded directory is deployed, recycle the WebFOCUS Application server.

The database table captures each security event in a separate row, as shown in the following image.

	USERID	DATETIME	LOGGER	MESSAGE
1	admin	2012-01-11 22:09:53,115	com.ibi.uoa.signin	signin SUCCESS user:admin monitorId:666c011363cd9...
2	admin	2012-01-11 22:12:37,727	com.ibi.uoa.signin	signin SUCCESS user:admin monitorId:6987fff8443e8d...
3	admin	2012-01-11 22:13:14,743	com.ibi.uoa.users	createUser SUCCESS user:shawshank (2065653048) s...
4	admin	2012-01-11 22:13:34,415	com.ibi.uoa.users	deleteUser SUCCESS user:abcdefghi (2065532905) sta...
5	admin	2012-01-11 22:16:31,058	com.ibi.uoa.signin	signin SUCCESS user:admin monitorId:6f9fcb1e85c6f3...

**Procedure: How to Save Sign-in Events in a Separate Log File**

1. Navigate to *drive:/ibi/WebFOCUS82/webapps/webfocus/WEB-INF/classes/*.
2. Open the *log4j2.xml* file, and go to the *<RollingFile name="LOGuoa">* block in the *<Appenders>* section.
3. Beneath the closing tag for the *LOGuoa* block, insert the following new *RollingFile* tag, which saves the sign-in events to a file named *signinout.log*, as shown in the following code example.

```

<RollingFile name="LOGuoaSignInOut">
  <FileName>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/signinout.log</FileName>
  <FilePattern>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/signinout-%d{yyyy-MM-dd}-%i.log</FilePattern>
  <PatternLayout>
    <Pattern>[%d] %-5p %-16.16c{1} %-16.16X{monitorID} %X{userId} %m
  %n</Pattern>
  </PatternLayout>
  <Policies>
    <TimeBasedTriggeringPolicy />
    <SizeBasedTriggeringPolicy size="20 MB" />
  </Policies>
</RollingFile>

```

4. Search within the file for the logger `name="com.ibi.uoa.signin"`, and update the entry to identify the new `LOGuoaSignInOut` appender block as the target of the appender reference, as shown in the following example.

```

<logger name="com.ibi.uoa.signin" level="info" additivity="false">
  <AppenderRef ref="LOGuoaSignInOut"/>
</logger>

```

5. Save the file.

Sign-in events are now recorded in the `signinout.log` file, which will appear in the All Clients list of traces.

### **Procedure: How to Save Sign-in Events in a Separate Database Table**

1. Create a new table in your database to capture the sign-in event records, as shown in the following example prepared for a PostgreSQL © database.

```

CREATE TABLE public.wf_log
(
  eventdate timestamp with time zone,
  logger character varying(128) COLLATE pg_catalog."default",
  level character varying(12) COLLATE pg_catalog."default",
  logid character varying(128) COLLATE pg_catalog."default",
  message character varying(255) COLLATE pg_catalog."default",
  exception text COLLATE pg_catalog."default"

GRANT UPDATE, INSERT, SELECT ON TABLE public.wf_log TO webfocus;

```

2. Navigate to `drive:/ibi/WebFOCUS82/webapps/webfocus/WEB-INF/classes/`.
3. Open the copy of the `drive:/ibi/WebFOCUS82/webapps/webfocus/WEB-INF/classes/log4j2.xml` file with a text editor.
4. Go to the `<RollingFile name="LOGuoa">` block in the `<Appenders>` section.
5. Beneath the closing tag for the `LOGuoa` block, insert a new JDBC tag, which saves the sign-in events to the database table using one of the following examples.

To transfer control of the connection to the external database, include a description of the `ConnectionFactory` class, as shown in the second line of the following example.

```
<JDBC name="LOGuaoSignInOut" tableName="public.wf_log">
  <ConnectionFactory
    class="com.ibi.log4j2.ConnectionFactory"
    method="getConnection" />
  <Column name="eventdate" isEventTimestamp="true" />
  <Column name="logger" pattern="%logger" isUnicode="false" />
  <Column name="level" pattern="%level" isUnicode="false" />
  <Column name="logid" pattern="%X{userId}" isUnicode="false" />
  <Column name="message" pattern="%message" isUnicode="false" />
  <Column name="exception" pattern="%ex{full}" isUnicode="false" />
</JDBC>
```

Or

To retain control of the connection within WebFOCUS, include a `DriverManager` tag, as shown in the following example.

```
<JDBC name="LOGuaoSignInOut" tableName="public.wf_log">
  <DriverManager
    connectionString="jdbc:postgresql://localhost:5432/WebFOCUS82"
    driverClassName="org.postgresql.Driver"
    username="webfocus"
    password="webfocus" />
  <Column name="eventdate" isEventTimestamp="true" />
  <Column name="logger" pattern="%logger" isUnicode="false" />
  <Column name="level" pattern="%level" isUnicode="false" />
  <Column name="logid" pattern="%X{userId}" isUnicode="false" />
  <Column name="message" pattern="%message" isUnicode="false" />
  <Column name="exception" pattern="%ex{full}" isUnicode="false" />
</JDBC>
```

**Note:** You can substitute the `LOGuaoSignInOut` name in these examples with another descriptive name of your own choosing. You must be sure to place the same name in the `AppenderRef` tag of the logger that will direct events to this new appender.

6. Search for the logger with the `name="com.ibi.uoa.signin"` tag, and update the entry to identify the new LOGevent JDBC class as the target of the appender reference, as shown in the following example.

```
<Logger name="com.ibi.uoa.signin" level="info" additivity="false">
  <AppenderRef ref="LOGuaoSignInOut"/>
```

**Note:** You can substitute the `LOGuaoSignInOut` name in these examples with another descriptive name of your own choosing. You must be sure to place the same name in the `name` tag of the appender that will receive events from this logger.

7. Save the file.

Sign-in events are now recorded in the public.wf\_log database table.

## Understanding Security Events

The following table lists the types of security events recorded for auditing by WebFOCUS.

Subject of Event	Description of Event	Type of Changes Logged	Logger Name in log4j.xml
config	Configuration	Changes to webfocus.cfg, license changes	com.ibi.uoa.config
content	Content	Create, update, delete	com.ibi.uoa.content
groups	Group	Create, update, delete	com.ibi.uoa.groups
ownership	Ownership	Change the owner of a resource	com.ibi.uoa.ownership
roles	Role	Create, update, delete	com.ibi.uoa.roles
rules	Rule	Create, update, delete	com.ibi.uoa.rules
shares	Sharing	Share, share with	com.ibi.uoa.shares
signin	Sign in	Sign-in, sign-out, expired session	com.ibi.uoa.signin
users	User	Create, update, delete, add to group, remove from group	com.ibi.uoa.users

## Understanding Configuration Events

In the following table, each log entry is composed of the following elements:

- ❑ Timestamp, in the format of YYYY-MM-DD hh:mm:ss,sss.
- ❑ Log level, such as INFO.
- ❑ Type of event being logged, in this case, a configuration event indicated by *config*.
- ❑ Monitor ID of the user who performed the action.
- ❑ Specific event being logged, in this case, configUpdate, a configuration update.

- ❑ Whether the action succeeds or fails, indicated by SUCCESS or FAILURE.
- ❑ Name of the file affected, typically webfocus.cfg.
- ❑ Name of the user performing the action.
- ❑ New value of the changed property.
- ❑ Old value of the changed property.

Event	Log entry
webfocus.cfg change	[YYYY-MM-DD hh:mm:ss,sss] INFO config monitor_ID user_ID updateConfig {SUCCESS FAILURE} file:file_name user:user_ID parameterName:parameter_name newValue:new_value oldValue:old_value
License key change	[YYYY-MM-DD hh:mm:ss,sss] INFO config monitor_ID user_ID updateConfig {SUCCESS FAILURE} file:license_key_file user:user_ID parameterName:parameter_name newKey:new_value newSite:site_code

Understanding Content Events

In the following table, each log entry is composed of the following elements:

- ❑ Timestamp, in the format of YYYY-MM-DD hh:mm:ss,sss.
- ❑ Log level, such as INFO.
- ❑ Type of event being logged, in this case, a content event indicated by *content*.
- ❑ Monitor ID of the user who performed the action.
- ❑ Specific event, for example, createFolder or putItem.
- ❑ Whether the action succeeds or fails, indicated by SUCCESS or FAILURE.
- ❑ Name of the user performing the action.
- ❑ Location of the content affected by the action.
- ❑ Fields altered by the action.



Event	Log entry
Folder is created	[ YYYY-MM-DD hh:mm:ss,sss] INFO content <i>monitor_ID user_ID</i> createFolder {SUCCESS FAILURE} user: <i>user_ID</i> folder: <i>IBFS_address</i>
Folder details are modified	[ YYYY-MM-DD hh:mm:ss,sss] INFO content <i>monitor_ID user_ID</i> putFolderProperties {SUCCESS FAILURE} user: <i>user_ID</i> folder: <i>IBFS_address</i>
Folder is deleted	[ YYYY-MM-DD hh:mm:ss,sss] INFO content <i>monitor_ID user_ID</i> delete {SUCCESS FAILURE} user: <i>user_ID</i> folder: <i>IBFS_address</i>
Folder is duplicated or copied and pasted	[ YYYY-MM-DD hh:mm:ss,sss] INFO content <i>monitor_ID user_ID</i> copyFolder {SUCCESS FAILURE} user: <i>user_ID</i> srcitem: <i>IBFS_address</i> dstitem: <i>IBFS_address_copy</i> [ YYYY-MM-DD hh:mm:ss,sss] INFO content <i>monitor_ID user_ID</i> putFolderProperties {SUCCESS FAILURE} user: <i>user_ID</i> folder: <i>IBFS_address</i>
Folder is moved	[ YYYY-MM-DD hh:mm:ss,sss] INFO content <i>monitor_ID user_ID</i> moveFolder {SUCCESS FAILURE} user: <i>user_ID</i> srcitem: <i>old_IBFS_address</i> dstitem: <i>new_IBFS_address</i>
Folder is renamed	[ YYYY-MM-DD hh:mm:ss,sss] INFO content <i>monitor_ID user_ID</i> putFolderProperties {SUCCESS FAILURE} user: <i>user_ID</i> folder: <i>new_IBFS_address</i>
Item is created	[ YYYY-MM-DD hh:mm:ss,sss] INFO content <i>monitor_ID user_ID</i> createItem {SUCCESS FAILURE} user: <i>user_ID</i> folder: <i>IBFS_address</i>
Item details are modified	[ YYYY-MM-DD hh:mm:ss,sss] INFO content <i>monitor_ID user_ID</i> putItem {SUCCESS FAILURE} user: <i>user_ID</i> item: <i>IBFS_address</i>
Item is deleted	[ YYYY-MM-DD hh:mm:ss,sss] INFO content <i>monitor_ID user_ID</i> delete {SUCCESS FAILURE} user: <i>user_ID</i> item: <i>IBFS_address</i>

Event	Log entry
Item is duplicated or copied and pasted	<pre>[ YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID copyItem {SUCCESS FAILURE} user:user_ID srcitem:old_IBFS_address dstitem:new_IBFS_address [ YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID putItemProperties {SUCCESS FAILURE} user:user_ID folder:IBFS_address</pre>

Understanding Group Events

In the following table, each log entry is composed of the following elements:

- ☐ Timestamp, in the format of YYYY-MM-DD hh:mm:ss,sss.
- ☐ Log level, such as INFO.
- ☐ Type of event being logged, in this case, a group event indicated by *groups*.
- ☐ Monitor ID of the user who performed the action.
- ☐ Description of the action, for example, createGroup or putGroup.
- ☐ Whether the action succeeds or fails, indicated by SUCCESS or FAILURE.
- ☐ Name and unique numeric ID of the group affected by the action.
- ☐ Fields altered by the action.

Each user and group is identified by a unique numerical ID, as well as by name.

Event	Log entry
Group is created	<pre>[ YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID createGroup {SUCCESS FAILURE} name:group_name (group_ID) parent:group_parent (parent_group_ID) desc:group_description extGrp:external_group_mappings</pre>
Group is deleted	<pre>[ YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID deleteGroup {SUCCESS FAILURE} group:IBFS_address (group_ID) users-autoremoved:number_of_group_members</pre>

Event	Log entry
Group description is modified	<code>[YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID putGroup {SUCCESS FAILURE} groupPath:IBFS_address (group_ID) newdesc:new_description olddesc:old_description externalGroups:external_group_mappings</code>
Group is renamed	<code>[YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID renameGroup {SUCCESS FAILURE} name:group_name (group_ID) parent:parent_group oldName:old_group_name</code>
User is added to group	<code>[YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID addUserToGroup {SUCCESS FAILURE} user:user_IDgroup:group_name (group_ID)</code>
User is deleted from group	<code>[YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID removeUserFromGroup {SUCCESS FAILURE} user:user_ID group:group_name (group_ID)</code>

## Understanding Library Access Events

In the following table, each log entry is composed of the following elements:

- ☐ Timestamp noting when the Library report was accessed, in the format of YYYY-MM-DD hh:mm:ss,sss.
- ☐ Log level, such as INFO.
- ☐ Thread Identifier, in the format of http-connector-port\_number-exec-ID\_number:libaccess.
- ☐ User ID of the user accessing the Library report.
- ☐ The full IBFS path of the Library report.
- ☐ The title of the Library report.
- ☐ The Version number of a Library report.

Event	Log entry
Library report is viewed.	[ YYYY-MM-DD hh:mm:ss,sss] INFO [Thread Identifier] User_ID - FullPath: IBFS_address ; Description: Library_Report_Title; Version Number: Library_Report_Version_Number

Understanding Magnify Console Events

The audit log records changes to values, index items, and options in the Magnify Console. For more information, see the *Magnify Search Security and Administration* technical content.

In the following table, each log entry is composed of the following elements:

- ☐ Timestamp, in the format of YYYY-MM-DD hh:mm:ss,sss.
- ☐ Log level, such as INFO.
- ☐ Type of event being logged, indicated by *magnify*.
- ☐ Monitor ID of the user who performed the action.
- ☐ User ID of the user who performed the action.
- ☐ IP Address of the user who performed the action.
- ☐ A unique description of the specific Magnify Console event. This description may span several lines depending on the amount of actions performed by the user.

Event	Log entry
Magnify Timers	

Event	Log entry
A user changed a setting on the Magnify Timers page. This log entry shows the timer option that has been changed on the Magnify Timers page and the new time setting for the timer option.	<p>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify <i>Monitor_ID User_ID User [User_ID]</i> and IP address [<i>IP address</i>] tried to reset [<i>timer option</i>] timer to [<i>new time setting</i>] on the Magnify Timers console page.</p> <p><b>Note:</b> To validate the successful completion of this activity, open the Magnify Timers page from the Magnify Console and review the current status of the changed Indexing Timers setting.</p>
A user changed the Reading Refresh Rate attribute. This log entry shows the True/False option that has been set for the Reading Refresh Rate.	<p>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify <i>Monitor_ID User_ID User [User_ID]</i> and IP address [<i>IP address</i>] tried to reset Reading Refresh Rate Enabled attribute to [<i>true/false</i>] on the Magnify Timers console page.</p> <p><b>Note:</b> To validate the successful completion of this activity, open the Magnify Timers page from the Magnify Console and review the current status and attribute of the Reading Refresh Rate.</p>
<b>Spell Check Setup</b>	
A user initiated the creation of or update to an Index Library Dictionary on the Spell Check Setup page. This log entry shows the specific index that was updated.	<p>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify <i>Monitor_ID User_ID User [User_ID]</i> and IP address [<i>IP address</i>] tried to create or update spell check dictionary for index [<i>index</i>] on Spell Check Setup console page.</p> <p><b>Note:</b> To validate the successful completion of this activity, open the Spell Check Setup page from the Magnify Console and review the status of the Index Library Dictionary identified in the entry. If the operation was successful, the entry reads, “<i>Dictionary up to date</i>”.</p>

Event	Log entry
A user initiated the creation of or update to a Collection Dictionary on the Spell Check Setup page. This log shows the specific collection that was updated.	<p>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify <i>Monitor_ID User_ID User [User_ID]</i> and IP address [<i>IP address</i>] tried to create or update spell check dictionary for collections [<i>collection</i>] on Spell Check Setup console page.</p> <p><b>Note:</b> To validate the successful completion of this activity, open the Spell Check Setup page from the Magnify Console and review the status of the Collection Dictionary identified in the entry. If the operation was successful, the collection will display the latest date and time it was updated.</p>
A user initiated the Close Dictionaries operation on the Spell Check Setup page.	<p>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify <i>Monitor_ID User_ID User [User_ID]</i> and IP address [<i>IP address</i>] tried to close dictionaries (for backup or removal) on Spell Check Setup console page.</p> <p><b>Note:</b> To validate the successful completion of this activity, open the Spell Check Setup page from the Magnify Console and review the status of the dictionary entry. If the operation was successful the entry reads, "Dictionary up to date".</p>
Analyzer Review	
A user initiated a text analysis on the Analyzer Review page. This log shows the specific text that was analyzed and the specific analyzer used to analyze the text.	<p>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify <i>Monitor_ID User_ID User [User_ID]</i> and IP address [<i>IP address</i>] tried to analyze [<i>text</i>] with analyzer [<i>analyzer</i>] on Analyzer Review console page.</p>
Collections Refresh	

Event	Log entry
<p>A user added a new daily refresh time to the Magnify Console Collections Refresh page. This log shows the hour:minute value of the new refresh time, and any additional comments added for the new refresh time.</p>	<pre>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID User [User_ID] and IP address [IP address] added a new daily refresh time on Collections Refresh console page. [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID User [User_ID] New refresh time is: [hour:minute] [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID User [User_ID] New refresh time comment is: [comment]</pre>
<p>A user initiated a collections refresh by reloading the index collections in the collections.xml file.</p>	<pre>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID User [User_ID] and IP address [IP Address] just refreshed collections file on Collections Refresh console page.</pre>
<p>A user removed a daily refresh time from the Magnify Console Collections Refresh page. This log shows the hour:minute value of the reviewed refresh time.</p>	<pre>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID User [User_ID] and IP address [IP Address] removed an existing daily refresh time on Collections Refresh console page. [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID The removed refresh time is: [hour:minute]</pre>
<b>IP Restrictions</b>	

Event	Log entry
A user modified data on the Magnify Console Feed Security Setup page. This log shows the latest host names, IPv4 addresses, and IPv6 addresses added to the Feed Security Setup page.	<pre>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID User [User_ID] and IP address [IP Address] modified the Feed Security Setup Console data to the following: [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID===== [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID Feed Security enable was set to: [true/false] [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID List of Host Names were set to: [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID [List of Host Names] [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID List of IPv4 Addresses were set to: [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID [List of IPv4 Addresses] [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID  List of IPv6 Addresses were set to: [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID [List of IPv6 Addresses] [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID=====</pre>
<b>Delete Indexes</b>	
A user deleted one or more indexes from the file system. This log shows the specific indexes that were deleted.	<pre>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID User [User_ID] and IP address [IP Address] tried to delete the following indexes: [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID ===== [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID [index] (index file path) [YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID=====</pre> <p><b>Note:</b> To validate the successful completion of this activity, open the Delete Indexes page from the Magnify Console and review the current list of indexes. If the operation was successful, the deleted index does not display.</p>
<b>Close Searchers and Readers</b>	
A user closed a searcher. This log shows the specific search file path of the search that was closed.	<pre>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify Monitor_ID User_ID User [User_ID] and IP address [IP Address] tried to close searcher for [search file path]</pre> <p><b>Note:</b> To validate the successful completion of this activity, open the Close Searchers and Readers page from the Magnify Console and review the current list of open searchers. If the operation was successful, the searcher does not display.</p>



Event	Log entry
A user closed an index reader. This log shows the specific datasource file path of the index reader that was closed.	<p>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify <i>Monitor_ID User_ID User [User_ID]</i> and IP address [<i>IP Address</i>] tried to close index reader for [<i>datasource file path</i>].</p> <p><b>Note:</b> To validate the successful completion of this activity, open the Close Searchers and Readers page from the Magnify Console and review the current list of open index readers. If the operation was successful, the index reader does not display.</p>
<b>Index Monitor</b>	
A user committed additional data to an index. This log shows the specific index writer file path of the index reader that has been closed.	<p>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify <i>Monitor_ID User_ID User [User_ID]</i> and IP address [<i>IP Address</i>] tried to commit on index writer [<i>index writer file path</i>].</p> <p><b>Note:</b> To validate the successful completion of this activity, open the Index Monitor page from the Magnify Console and review the index stated to be committed. If the operation was successful, the commit count number for the index library will have increased by the number of times the commit was stated to have been performed.</p>
<b>Servlet Form</b>	
A user successfully loaded a record to a specific index.	<p>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify User [<i>User_ID</i>] and IP address [<i>IP Address</i>] successfully loaded a record to index [<i>index</i>] from the Servlet Form page in the Magnify Console.</p> <p><b>Note:</b> To validate the successful completion of this activity, contact the user to confirm whether the magnify feed response was received.</p>

Event	Log entry
A user tried to verify a record against a datasource. This log shows the specific datasource that has been verified, and the unique value which designates the datasource.	<p>[YYYY-MM-DD hh:mm:ss,sss] INFO magnify <i>Monitor_ID</i> <i>User_ID</i> User [<i>User_ID</i>] and IP address [<i>IP Address</i>] tried to verify a record with datasource [<i>datasource</i>] and WF_INDEX_UNIQUE_KEY [<i>a_unique_value</i>]</p> <p><b>Note:</b> To validate the successful completion of this activity, contact the user to confirm whether the magnify feed response was received.</p>

## Understanding Ownership Events

In the following table, each log entry is composed of the following elements:

- ☐ Timestamp, in the format of YYYY-MM-DD hh:mm:ss,sss.
- ☐ Log level, such as INFO.
- ☐ Type of event being logged, in this case, an ownership event indicated by *ownership*.
- ☐ The action taken, such as a change of ownership, indicated by *changeOwner*, or the publication of an item, indicated by *makePublic*.
- ☐ Whether the action succeeds or fails, indicated by SUCCESS or FAILURE.
- ☐ Whether the resource inherits its privacy from its parent.
- ☐ The full IBFS path of the resource.
- ☐ User ID of the new resource owner.
- ☐ Type of owner, G for a group or U for a user.

Event	Log entry
Change owner to group	<p>[YYYY-MM-DD hh:mm:ss,sss] INFO ownership <i>monitor_ID</i> <i>user_ID</i> makeManaged {SUCCESS FAILURE} inherited:{TRUE FALSE} strPath:<i>IBFS_address</i> ownerName:<i>owner_group_name</i> ownerType:G</p>

Event	Log entry
Change owner to user	[YYYY-MM-DD hh:mm:ss,sss] INFO ownership <i>monitor_ID user_ID</i> changeOwner {SUCCESS FAILURE} inherited:{TRUE FALSE} strPath: <i>IBFS_address</i> ownerName: <i>owner_user_ID</i> ownerType:U
Folder or item is made private	[YYYY-MM-DD hh:mm:ss,sss] INFO ownership <i>monitor_ID user_ID</i> makePrivate {SUCCESS FAILURE} strPath: <i>IBFS_address</i> ownerName: <i>new_owner</i> ownerType:U
Folder or item is published	[YYYY-MM-DD hh:mm:ss,sss] INFO ownership <i>monitor_ID user_ID</i> makePrivate {SUCCESS FAILURE} strPath: <i>IBFS_address</i> ownerName: <i>new_owner</i> ownerType:U
Folder or item fails to be published	[YYYY-MM-DD hh:mm:ss,sss] INFO ownership <i>monitor_ID user_ID</i> isPublishable {SUCCESS FAILURE} inherited:{TRUE FALSE} ownerName: <i>parent_folder</i>

## Understanding ReportCaster Configuration Events

In the following table, each log entry is composed of the following elements:

- ☐ Timestamp, in the format of YYYY-MM-DD hh:mm:ss,sss.
- ☐ Log level, such as INFO.
- ☐ Type of event being logged, in this case, a ReportCaster Configuration event indicated by *caster\_config*.
- ☐ Monitor ID of the user who performed the action.
- ☐ Name of the user who performed the action.
- ☐ Name of the file affected, typically, the old CasterConfig file.

Event	Log entry
ReportCaster Configuration settings are edited and saved	<code>[YYYY-MM-DD hh:mm:ss,sss] INFO caster_config monitor_ID user_ID updated ReportCaster configuration, old CasterConfig file: dserver_file_ID.xml</code>

**Note:** Before changes to the ReportCaster Configuration settings are saved, the previous settings of the ReportCaster Configuration tool are written to a timestamped dserver.xml file. This file is saved in the ...ibi\WebFOCUSnn directory, where nn is the WebFOCUS release number.

Understanding ReportCaster Global Update Events

The globalUpdates log records global changes to values stored in ReportCaster schedules and certain scheduling tools, using the Global Updates command. For more information, see the *ReportCaster* technical content.

In the following table, each log entry is composed of the following elements:

- ❑ User ID of the user initiating the global update event.
- ❑ Name of the database table targeted by the global update.
- ❑ Name of the updated variable.
- ❑ Old Value that was globally removed.
- ❑ New Value that was globally added.
- ❑ Thread Identifier, in the format of *ID\_number*.

Event	Log entry
Value was globally updated.	<code>User_ID database table name variable name old value new value Thread Identifier</code>

## Understanding Role Events

In the following table, each log entry is composed of the following elements:

- ☐ Timestamp, in the format of YYYY-MM-DD hh:mm:ss,sss.
- ☐ Log level, such as INFO.
- ☐ Type of event being logged, in this case, a role event indicated by *roles*.
- ☐ Monitor ID of the user who performed the action.
- ☐ User ID of the user who performed the action.
- ☐ Specific event, for example, createRole.
- ☐ Whether the action succeeds or fails, indicated by SUCCESS or FAILURE.
- ☐ Name of the role affected by the action.
- ☐ Policy for the role.

Event	Log entry
Role is created	<code>[ YYYY-MM-DD hh:mm:ss,sss] INFO roles monitor_ID user_ID createRole {SUCCESS FAILURE} role:role_name (role_ID) desc:description policy:privilege_name:OPERATION;</code>
Role details are modified	<code>[ YYYY-MM-DD hh:mm:ss,sss] INFO roles monitor_ID user_ID putRole {SUCCESS FAILURE} role:role_name (role_ID) desc:description policy:privilege_name:OPERATION;</code>
Role is deleted	<code>[ YYYY-MM-DD hh:mm:ss,sss] INFO roles monitor_ID user_ID deleteRole {SUCCESS FAILURE} role:role_name (role_ID) rules-autoremoved:number_rules_using_this_role policy:privilege_name:OPERATION;</code>
Role is cloned	<code>[ YYYY-MM-DD hh:mm:ss,sss] INFO roles monitor_ID user_ID createRole {SUCCESS FAILURE} role:role_name_copy (role_ID) desc:description_copy policy:privilege_name:OPERATION;</code>

## Understanding Rule Events

In the following table, each log entry is composed of the following elements:

- ☐ Timestamp, in the format of YYYY-MM-DD hh:mm:ss,sss.

- ☐ Log level, such as INFO.
- ☐ Type of event being logged, in this case, a rule event indicated by *rules*.
- ☐ Monitor ID of the user who performed the action.
- ☐ User ID of the user who performed the action.
- ☐ Specific event, for example, addGroupRule or addUserRule.
- ☐ Whether the action succeeds or fails, indicated by SUCCESS or FAILURE.
- ☐ Location of the resource to which the rule applies.
- ☐ Access policy of the rule.
- ☐ Whether the rule applies to this location only, the children of this location only, or to this location and its children.

Event	Log entry
Rule is created for a group	[ YYYY-MM-DD hh:mm:ss,sss] INFO rules monitor_ID user_ID addGroupRule {SUCCESS FAILURE} group_name (group_ID) role:IBFS_address (role_ID) resource:resource_location (resource_ID) verb:operation applyTo:scope
Rule is created for a user	[ YYYY-MM-DD hh:mm:ss,sss] INFO rules monitor_ID user_ID addUserRule {SUCCESS FAILURE} user_ID (numeric_user_ID) role:IBFS_address (role_ID) resource:resource_location (resource_ID) verb:operation applyTo:scope

Understanding Sharing Events

- ☐ Timestamp, in the format of YYYY-MM-DD hh:mm:ss,sss.
- ☐ Log level, such as INFO.
- ☐ Type of event being logged, in this case, a sharing event indicated by *shares*.
- ☐ Monitor ID of the user who performed the action.
- ☐ User ID of the user who performed the action.
- ☐ Specific event, for example, clearShares.

- ☐ Whether the action succeeds or fails, indicated by SUCCESS or FAILURE.
- ☐ Whether the owner of the resource is a group or an individual user, G or U.
- ☐ The owner ID.

Event	Log entry
Resource is shared or shared with	<code>[ YYYY-MM-DD hh:mm:ss,sss] INFO shares monitor_ID user_ID {SUCCESS FAILURE} setShares resource:IBFS_address count:number_of_parties_shared_with ownerType:{G U} ownerID:owner_ID</code>
Resource is unshared	<code>[ YYYY-MM-DD hh:mm:ss,sss] INFO shares monitor_ID user_ID clearShares {SUCCESS FAILURE} resource:IBFS_address count:number_of_parties_shared_with ownerType:{G U} ownerID:owner_ID</code>

## Understanding Sign-in Events

In the following table, each log entry is composed of the following elements:

- ☐ Timestamp, in the format of YYYY-MM-DD hh:mm:ss,sss.
- ☐ Log level, such as INFO.
- ☐ Type of event being logged, in this case, a sign-in event indicated by *signin*.
- ☐ Monitor ID of the user who performed the action.
- ☐ User ID of the user who performed the action.
- ☐ Description of the action, for example, *signIn*.
- ☐ Whether the action succeeds or fails, indicated by SUCCESS or FAILURE.
- ☐ Name and monitor ID of the user who signed in.
- ☐ The IP address and user agent or type of browser, if available.

Each user is identified by a unique numerical ID, as well as by name.

Event	Log entry
User signs in	[ YYYY-MM-DD hh:mm:ss,sss] INFO signin monitor_ID user_ID signIn {SUCCESS FAILURE} user:user_ID monitorId:monitor_ID IPaddr:IP_address userAgent:user_agent userDescription:user_description sessionType:session_type
User signs out	[ YYYY-MM-DD hh:mm:ss,sss] INFO signin monitor_ID user_ID signOut {SUCCESS FAILURE} user:user_ID monitorId:monitor_ID
User session expires	[ YYYY-MM-DD hh:mm:ss,sss] INFO signin monitor_ID user_ID signOut {SUCCESS FAILURE} user:user_ID monitorId:monitor_ID

**Reference:** Understanding WebFOCUS Reporting Server Authentication Failure Messages

If the External Security Type (IBI\_AUTHENTICATION\_TYPE) setting is Reporting Server, and WebFOCUS Reporting Server authentication fails, the end user always sees a generic failure message. However, the audit log captures more descriptive errors, as detailed in the table below.

Description	Return Code
Invalid user ID or password.	ERROR_AUTHENTICATION_FAILURE(5003)
Credentials are valid, but the user ID is inactive.	ERROR_AUTHENTICATION_FAILURE_ID_INACTIVE(5006)
Credentials are valid, but the user must change the password.	ERROR_AUTHENTICATION_MUST_CHANGE_PASSWORD(5007)
Credentials are valid, but the password has expired.	ERROR_AUTHENTICATION_PASSWORD_EXPIRED(5008)
Credentials are valid, but the user has surpassed the allowed number of sign-in attempts (specified in the IBI_Max_Bad_Attempts setting).	ERROR_AUTHENTICATION_USER_LOCKED(5009)
Credentials are valid, but the user is still signed in to a prior session.	ERROR_AUTHENTICATION_USER_ALREADY_LOGGED_IN(5020)



**Reference: Understanding User Sign-in Error Messages**

The following table lists the error messages for when a sign-in attempt or password change is unsuccessful.

Event	Failure Message
User does not exist in the repository.	<code>signIn Failure-unregistered_user User:xyzabc</code>
User exists in the repository, but not on the Reporting Server.	<code>signIn Failure-EDA-RC User:admin RC:32033 EDANODE:EDASERVE</code>
User exists in the repository and Reporting Server, but the password entered is invalid.	<code>signIn Failure-EDA-RC User:bn01618 RC:32034 EDANODE:EDASERVE</code>
User exists in the repository and Reporting Server, but the account has been disabled.	<code>signIn Failure-Unknown User:cssadmin RC:32063 EDANODE:EDASERVE</code>
User exists in the repository and Reporting Server, but the password must be changed.	<code>signIn Failure-EDA-RC User:cssadmin RC:32034 EDANODE:EDASERVE</code>

**Procedure: How to Troubleshoot a Database Connection Failure**

1. Check that your database is running.

If you have installed Derby, check that it is listening on the default port of 1527 and determine its network interface. You can use the `netstat -an` command. Possible results are listed below.

Local Address	Description
0.0.0.0	Port is listening on all network interfaces.
127.0.0.1	Port is listening only for connections from your computer.
Your IP address	Port is listening only for connections on that interface.

2. Check the `audit.log` file for errors.

- 3. If the audit.log file indicates that the administrative user is unregistered, but this is a new installation with the default administrative user, consult the event log file for specific errors regarding the registration of this user.

The event log file contains specific database connectivity errors. It will show the following relevant information:

- ☐ Whether Managed Reporting can connect to the database at all.
- ☐ Whether the database tables have been created.
- ☐ Whether the database tables have been populated with data.

Understanding  
User Events

In the following table, each log entry is composed of the following elements:

- ☐ Timestamp, in the format of YYYY-MM-DD hh:mm:ss,sss.
- ☐ Log level, such as INFO.
- ☐ Type of event being logged, in this case, a user event indicated by *users*.
- ☐ Monitor ID of the user who performed the action.
- ☐ Description of the action, for example, createUser or putUser.
- ☐ Whether the action succeeds or fails, indicated by SUCCESS or FAILURE.
- ☐ User ID and unique numeric ID of the user affected by the action.
- ☐ Fields altered by the action.

Each user and group are identified by unique numerical IDs, as well as by name.

Event	Log entry
User is created	<code>[ YYYY-MM-DD hh:mm:ss,sss] INFO users monitor_ID user_ID createUser {SUCCESS FAILURE} user:user_ID (user_number) status:{ACTIVE INACTIVE} email:email_address desc:description</code>
User details are modified	<code>[ YYYY-MM-DD hh:mm:ss,sss] INFO users monitor_ID user_ID putUser {SUCCESS FAILURE} userName:user_name Seat-Type-Property:property</code>

Event	Log entry
User account is disabled	<code>[ YYYY-MM-DD hh:mm:ss,sss] INFO users monitor_ID user_ID putUser {SUCCESS FAILURE} user:user_ID (user_number) status:INACTIVE email:email_address desc:description</code>
User account is deleted	<code>[ YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID removeUserFromGroup {SUCCESS FAILURE} user:user_ID (user_number) group:group_name (group_ID) [ YYYY-MM-DD hh:mm:ss,sss] INFO deleteUser monitor_ID user_ID status:{ACTIVE INACTIVE} email:email_address desc:description</code>
Password is changed	<code>[ YYYY-MM-DD hh:mm:ss,sss] INFO users changePassword {SUCCESS FAILURE} user:user_whose_password_is_changed (user_number) status:{ACTIVE INACTIVE} email:email_address desc:description</code>

## Understanding Monitor Logs

Monitor logs capture records of system performance once every minute.

For security purposes, monitor logs are always enabled. By default, the monitor logs are saved for ten days on the WebFOCUS Client. You can customize the amount of time for which logs are saved, save sign-in events to a separate log, and save logs to a database.

## Understanding a Monitor Log Event

Monitor log events record system performance statistics at specified dates and times. Monitor log entries created during these events list the date and time at which the record was captured, followed by the statistics and values recorded during the event.

In the table and deception below all times are in milliseconds, and all file sizes are in kilobytes (KB), unless otherwise specified.

Each monitor log record takes the following format:

Event	Log entry
Monitor log capture	<code>[ YYYY-MM-DD HH:MM:SS,sss] INFO ActLog Sessions= n ActRecentSes= n SrvReq= n SrvTime= ms maxSrvRsp= ms SrvDbmsReq= n SrvDbmsTime= ms maxSrvDbmsRsp= ms maxConcur= n UrlReq= n UrlTime= ms maxUrlRsp= ms ClientCPU= ms maxClientCPU= ms dummy= n dummy= n dummy= n numSRVLogs= n numURLLogs= n minHeapAvail= kb minNonHeapAvail= kb maxPendFinalization= n CpuLoad= n JavaCpuLoad= n ActUrlSes= n ActUrls= n ActLongRunUrls= n ActSrvReqSes= n ActSrvReq= n ActLongRunSrvReq= n</code>

where:

`[ YYYY-MM-DD HH:MM:SS,sss]`

Is the date and time of the monitor event record. All statistics captured by the event were current as of this date and time.

`INFO`

Is the Log level, such as INFO. For more information see, [Working With Log Files](#) on page 201.

`ActLog`

Is the type of event being logged. In this case, an activity log record capture, identified by ActLog.

`Sessions= n`

Is the number of all sessions that were active during the previous minute. This number includes active and inactive sessions.

`ActRecentSes= n`

Is the number of sessions that were open *and* active, during the previous minute. This value is a subset of the Sessions value.

`SrvReq= n`

Is the total number of Reporting Server requests that occurred during the past minute.

`SrvTime= ms`

Is the total time, in milliseconds, of all Reporting Server requests that occurred during the previous minute.

`maxSrvRsp= ms`

Is the time of the longest Reporting Server Response, in milliseconds, that occurred during the previous minute.

`SrvDbmsReq= n`

Is the number of requests to access the external RDBMS that occurred during the previous minute. This value is a subset of the `SrvReq` value, which counts the total number of requests to the Reporting Server.

`SrvDbmsTime= ms`

Is the total time, in milliseconds, spent executing requests to the external RDBMS, during the previous minute.

`maxSrvDbmsRsp= ms`

Is the time, in milliseconds, of the longest RDBMS request executed during the previous minute. This value is a subset of the `SrvDbmsTime` value, which counts the total amount of time spent executing requests to the external RDBMS.

`maxConcur= n`

Is the total number of concurrent Reporting Server connections that were open during the previous minute.

`UrlReq= n`

Is the number of URL Requests during the previous minute.

`UrlTime= ms`

Is the total amount of time, in milliseconds, required to execute all URL requests during the previous minute.

`maxUrlRsp= ms`

Is the time required to execute the longest URL Response message during the previous minute.

`ClientCPU= ms`

Is the total amount of CPU time, in milliseconds, required to execute all URL requests during the previous minute.

`maxClientCPU= ms`

Is the maximum amount of Client CPU time required to execute the longest URL request during the previous minute.

`dummy= n`

Is a placeholder parameter. Disregard this parameter and its value.

`dummy= n`

Is a placeholder parameter. Disregard this parameter and its value.

`dummy= n`

Is a placeholder parameter. Disregard this parameter and its value.

`numSRVLogs= n`

Is the total number of logs of server requests and responses that were open during the previous minute.

`numURLLogs= n`

Is the total number of logs of URL requests and responses that were open during the previous minute.

`minHeapAvail= kb`

Is the minimum amount, in kilobytes, of memory available in the Java Virtual Machine Heap.

`minNonHeapAvail= kb`

Is the minimum amount, in kilobytes, of additional memory in the Java Virtual Machine.

`maxPendFinalization= n`

Is the maximum number of processes that were incomplete during the previous minute.

`CpuLoad= n`

Is a measure of CPU usage for the whole system during the previous minute. Values range from 0.0, meaning that all CPUs were idle, to 1.0, meaning that all CPUs were active for the entire minute. If recent CPU usage is not available, this parameter contains a negative value.

`JavaCpuLoad= n`

Is a measure of CPU usage for the Java Virtual Machine (JVM) process during the previous minute. Values range from 0.0, meaning that none of the CPUs were running threads from the JVM process, to 1.0, meaning that all CPUs were actively running threads from the JVM process for the entire minute. If recent CPU usage for the JVM process is not available, this parameter contains a negative value.

`ActUrlSes= n`

Is the number of sessions that currently have an active URL.

`ActUrls= n`

Is the number of currently active URLs.

`ActLongRunUrls= n`

Is the number of currently active long-running URLs.

`ActSrvReqSes= n`

Is the number of sessions that currently have an active Reporting Server connection.

`ActSrvReq= n`

Is the number of currently active server requests.

`ActLongRunSrvReq= n`

Is the number of currently active long running Reporting Server connections.

## Understanding the Monitor ID

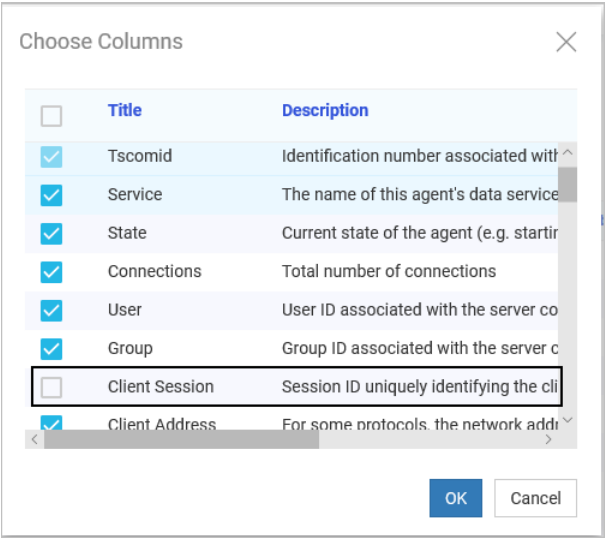
A monitor ID is a unique, randomly-generated identifier created for each client session. The monitor ID allows an administrator to reference sessions without exposing individual user application server session IDs. It acts as a unique identifier for each user from a specific location, allowing you to distinguish among multiple people signed in under the same user ID, such as *public* or *admin*. By default, the monitor ID is passed on to the Reporting Server, but is not displayed in the Reporting Server Console.

Each independent sign-in to WebFOCUS Express is identified by a unique 64-character internal IBFS session ID. The monitor ID, which is the first fifteen characters of the IBFS session ID, is passed on to the Reporting Server, where it is used to identify the temporary file foccache location for each user on the Reporting Server for the current session.

The monitor ID appears in many WebFOCUS Express logs, including the session monitor log, the trace log, and the security logs. You can view these logs from the Log files page in the Diagnostics tab of the Administration Console.

You can view live individual sessions, enable trace logging, request logging, or procedure logging for an individual sessions from the Session Monitor page in the Diagnostics tab of the Administration Console.

To display the monitor ID in the Reporting Server Console, you must activate a column for it. To do so, open the Reporting Server Console, select *Tools* and select *Workspace*. On the *Workspace* tab, in the *Monitor* group, click *Data Service Agents*. In the *Data Services Agents* page, select *Choose Columns* from the shortcut menu. In the column selection dialog box, select the *Client Session* check box, as shown in the following image, and then click *OK*.



## Understanding Change Management Import and Export Logs

Change Management Import and Export Logs capture events that take place during change management export and import operations. The system events and messages they record support your review of change management activities and change management problem condition troubleshooting.

The `cm_export` log and `cm_import` log links appear in the Logs column of the Log Files page, located on the Diagnostics tab of the Administration Console.

In both logs, entries are listed in order, from earliest to most recent, and each log covers the activities of a single day. By default, these logs are set to the `DEBUG` trace level, but administrators can adjust this trace level to increase or decrease the level of detail captured by the log.

Log entries are composed of the following elements:

- ☐ Date, in the format of `YYYY-MM-DD HH:MM:SS:SSS`.
- ☐ Log Level, such as `DEBUG`.



- ❑ Requester URL:operation (import or export), in the format [http-host-port-directory-file:operation]. For example, [http-nio-8080-exec-5:import].
- ❑ User ID.
- ❑ System Event or message.

For example:

```
[2018-08-17 08:33:32,987] DEBUG [http-nio-8080-exec-4:export] admin -
ExportData - addResource: "IBFS:/WFC/Repository/HealthcareNet"
```

## Export Package Created By Entry

In the cm\_import log, the Export package generated by user log entry captures the identity of the user who created an import package as shown in the following example.

```
[2018-08-17 09:08:50,614] INFO [http-nio-8080-exec-2:import] admin -
Export package generated by user: admin
```

This entry appears after the list of import operation parameters that follows the START IMPORT Process entry. However, to capture this entry, the cm\_import log must be set to the INFO trace level.

## Understanding the Advanced Web Tools, BI Portal, Event, EclipseLink JPA, and ReportCaster Log

All activities from the InfoAssist tool, BI Portal, and ReportCaster are tracked and appended to the log file named event.log, which is located in the *drive:/ibi/WebFOCUS82/logs* directory. The following log levels are available:

- ❑ **OFF.** No activity is written to the log file.
- ❑ **FATAL.** Produces minimum tracing.
- ❑ **ERROR.** Logs information only if an error occurs.
- ❑ **WARN.** Captures only warning messages.
- ❑ **INFO.** Captures only informational messages.
- ❑ **DEBUG.** Produces maximum tracing.
- ❑ **TRACE.** Enables tracing.

**Note:** When setting the log level for org.eclipse.persistence to DEBUG or TRACE, the event.log file will contain tracing information that includes a list of the bound parameters for SQL queries.

## Diagnostics

---

This topic explains how to enable the diagnostic traces available for the WebFOCUS Client.

Traces can be generated and viewed in the Administration Console for the Servlet implementation of the WebFOCUS Client. Each of these traces can be turned on and off on its trace page. Only administrators can enable traces. Internal password variables are masked when written to trace files or logs.

Because it can affect performance, tracing is only recommended for troubleshooting as it affects performance. When you are confident that you have configured WebFOCUS properly, turn traces off and reload your web application.

To access the trace files, open the Session Viewer. You can view traces from individual sessions on screen or zip copies of them for review in trace file format. For more information, see [Viewing Sessions](#) on page 186.

### In this appendix:

- ☐ [Understanding All Clients Traces](#)
  - ☐ [Understanding Client Connector Traces](#)
  - ☐ [Understanding Monitor Log Traces](#)
  - ☐ [Understanding Web Security Traces](#)
  - ☐ [Understanding Web Services Traces](#)
  - ☐ [Understanding WFServlet Traces](#)
- 

### Understanding All Clients Traces

Selecting the *All Clients* trace option, rather than one particular trace, displays a list of all trace files for all activated traces.

### Understanding Client Connector Traces

This traces Client connections to the Reporting Server. The type of trace that appears (NGXXJ or JLINK) depends on the IBI\_EDACONNECTOR setting.

Trace file names are of the following form:

*sequencenumber\_tracetype\_Connector\_date\_time.trace*

where:

*sequencenumber*

A new sequence number is generated with every trace file that gets created and helps determine the order of processing when reviewing traces for more than one component.

*tracetype*

Is the type of trace, NGXXJ or JLINK.

*date\_time*

Is the date and time the file was created.

**Note:** This setting updates the CONNECTOR\_TRACE setting in the Startup Parameters section of the Configuration section of the Administration Console. However, setting TRACE=ON overrides the CONNECTOR\_TRACE setting. When TRACE=ON is set, the Client Connector trace information is included within the trace file of the component (for example, WFServlet) that uses the WebFOCUS Express API (WFAPI) to make use of the Client Connector.

## Understanding Monitor Log Traces

The Monitor Log trace provides information about one or more active sessions. Logging is enabled using the tracing features on the Session Monitor page of the Administration Console Diagnostic tab or in the Session Viewer. You can enable traces for all sessions or for selected individual sessions. The Monitor log provides the following levels of diagnostic information:

- ☐ **OFF.** No information is written to the monitor.log file.
- ☐ **FATAL.** Produces minimum tracing.
- ☐ **ERROR.** Logs information only if an error occurs.
- ☐ **WARN.** Captures only warning messages.
- ☐ **INFO.** Captures only informational messages.
- ☐ **DEBUG.** Produces maximum tracing.
- ☐ **TRACE.** Enables tracing.

The information that is written to the log file is based on the log level that is set. For example, the INFO log level provides the following information in the log:

```
[YYYY-MM-DD hh:mm:ss,sss] INFO ReqEnd MonID=monitor_ID
ClientUser=user_ID ReqID=16.29.03.987-1 Node=node ServerUser=
Completed=completion_time
TimeUsed=time_to_run_request ReqInfo=request_information
```

where:

**MonID**

Is a unique identifier for each session.

**ClientUser**

Is the user ID that is running the request.

**ReqID**

Is a unique request identifier for the Reporting Server.

**Node**

Is the name of the Reporting Server that is running the request.

**ServerUser**

Is the Reporting Server user ID.

**Completed**

Is the time, in milliseconds, in which the request was complete.

**TimeUsed**

Is the length of time, in milliseconds, that it took to run the request.

**ReqInfo**

Provides information about the request, such as the application name and the report procedure name.

Log levels are usually set to INFO. DEBUG is the level recommended for troubleshooting.

## Understanding Web Security Traces

The Web Security Trace tracks validation requests affected by the Validation Settings. Log level options are:

- ☐ **OFF.** No information is written to the monitor.log file.
- ☐ **FATAL.** Produces minimum tracing.
- ☐ **ERROR.** Logs information only if an error occurs.

- ☐ **WARN.** Captures only warning messages.
- ☐ **INFO.** Captures only informational messages.
- ☐ **DEBUG.** Produces maximum tracing.
- ☐ **TRACE.** Enables tracing.

## Understanding Web Services Traces

Web services allow you to develop applications in the .NET or Java environments and perform WebFOCUS Express functionality from those environments.

Each trace file is a separate Web Service function call which traces the SOAP messages. This is important when programmers want to debug their .NET or Java programs when calling WebFOCUS web service functions.

**Note:** You can view Web Services traces from the Session Viewer or the Session Monitor.

## Understanding WFServlet Traces

The WFServlet trace tracks requests processed by the WFServlet implementation of the WebFOCUS Client. The trace file name takes the form:

*sequencenumber\_WFServlet\_WFAPI\_date\_time.trace*

A new sequence number is generated with every trace file that gets created. The date and time portions specify the date and time the file was created.

To enable WFServlet traces, select the Details option from the Trace Control list in the Session Monitor, or select the Details option from the Tracing Level list in the Session Viewer.

## Privileges

The following topic describes each of the privileges available when editing or creating a user role. The subsystem column defines the folders to which the privileges apply. Some privileges listed in this appendix are tied to licenses and configuration settings. They do not appear in the Security Center Role dialog box unless their affiliated license or configuration settings are in use.

**In this appendix:**

- ☐ [Basic Reporting](#)
- ☐ [Advanced Reporting](#)
- ☐ [Scheduling and Distribution](#)
- ☐ [Application Development](#)
- ☐ [Desktop Development](#)
- ☐ [Group Administration](#)
- ☐ [Administration](#)

### Basic Reporting

The following privileges can be assigned to most users, including those with minimal training. All of the other sets of privileges are granted in addition to the basic reporting features.

Privilege	Description	Subsystems	Privilege ID
Access Comments	User can view comments on content.	WFC	opReadComments
Access Library Content	User can view the library output distributed by ReportCaster.	Session, WFC	opLibrary
Access Portal	User can view defined portals.	WFC, BIP	opViewPortal

Privilege	Description	Subsystems	Privilege ID
Access Resource	User can view resources (required in most roles).	*	opList
Access Resource Properties	User can view the properties of a folder or an item.	WFC	opViewProps
Create Comments	User can create comments on content.	WFC	opCreateComments
Create Shortcuts	User can create shortcuts.	Session, WFC	opShortcut
Display About TIBCO WebFOCUS	Displays the <i>About TIBCO WebFOCUS</i> and <i>Licenses</i> options in the Help menu, so users can see version and environmental information.	Session	opDisplayVersionInfo
Display Ask TIBCO WebFOCUS for InfoSearch	Displays the Ask TIBCO WebFOCUS option on the sidebar where users can search for content.	Session	opInfoSearch
Display Ask TIBCO WebFOCUS for Mobile Voice	Displays Ask TIBCO WebFOCUS on the side bar where users can access voice-enabled content.	Session	opMobileVoice
Display Favorites Node	Displays the Favorites node in the Resource tree.	Session, WFC	opFavorites
Display Magnify Search Page	Displays the <i>Magnify Search Page</i> option in the Tools menu, so users can search TIBCO WebFOCUS content.	Session	opMagnify
Display Search	Displays the <i>Search</i> option in the shortcut menu of top-level folders, so users can find TIBCO WebFOCUS resources.	Session	opRepositorySearch



Privilege	Description	Subsystems	Privilege ID
Display Stop Requests	Displays the <i>Stop Requests</i> option in the Tools menu, so users can cancel submitted report requests.	Session	opStopRequests
Edit Comments	User can edit and delete their own comments on content.	WFC	opEditComments
Mobile Faves Email Option	User can email from the Mobile Faves App for iOS or Android.	WFC	opMobileFavesEmail
Mobile Faves Print Option	User can print from the Mobile Faves App for iOS or Android.	WFC	opMobileFavesPrint
Mobile Faves Save Option	User can save content to their own device from the Mobile Faves App for iOS or Android.	WFC	opMobileFavesSave
My Content Folder	TIBCO WebFOCUS creates a My Content folder for the user within the folders that have the <i>Auto Create My Content Folders</i> property selected.	WFC	opCreateMyFolder
Run Resources	User can run resources including reports, graphs, pages, and schedules and can access static content.	WFC, EDA	opRun
Run Procedures Deferred	User can submit reports and graphs for deferred processing.	Session, WFC	opRunDef

Privilege	Description	Subsystems	Privilege ID
Run Procedures with Different Connection Credentials	User can provide different credentials for data connections configured with the Prompt for Connections Credentials option.  <b>Note:</b> This privilege is visible only when the Prompt for Connection Credentials Option check box, located on the Other Settings page of the Administration Console, is selected.	WFC, EDA	opRunAs
Run Procedures with Insight	User can run graphs in an interactive canvas mode that allows quick ad hoc queries.	WFC	opRunEnhanced
Save Deferred Output	User can save deferred output to own My Content folder or to any writeable location.	Session	opSaveDef
Save Portal Customization	User can save own customized view of the portal.	WIF, BIP	opCustomizePortal
Save Procedure Parameters	User can save parameter selections for procedures.	WFC	opParmrpt

## Advanced Reporting

The following privileges can be assigned to users who need to create and share their own reports. They are generally granted as a supplement to the basic reporting privileges, not as a replacement for them.

Privilege	Description	Subsystems	Privilege ID
Create Alerts	User can create alerts that conditionally run reports.	WFC	opAlertAssistant

Privilege	Description	Subsystems	Privilege ID
Create URL Reports	User can create reports that reference URLs on the web.	Session, WFC	opURL
Data Visualization from Metadata	User can use the Data Visualization tool with the metadata selection dialog.	WFC	opVisualization
Designer Workbook	User can use Designer to create workbooks with embedded content.	Session, WFC	opWorkbookDesigner
Designer Content from Metadata	User can use Designer to create content from metadata.	Session, WFC	opDesignerMetadata
Designer Content from Business View	User can use Designer to create content from business views.	Session, WFC	opDesignerBV
Designer Content from Reporting Object	User can use Designer to create content from reporting objects.	Session, WFC	opDesignerReportingObject
Designer Page	User can use Designer to create pages (dashboards, InfoApps).	Session, WFC	opAppDesigner
Display Easel.ly Link	WebFOCUS displays Easel.ly Infographics in the Tools menu.	Session, WFC	opEaselly
Express Analytics	User can use the Express Analytics Engine to create reports, charts, and dashboards.	WFC	opExpressAnalytics
InfoAssist from Metadata	User can use InfoAssist with the metadata selection dialog.	WFC	opInfoAssist
InfoAssist from Reporting Object	User can use InfoAssist with Reporting Objects.	WFC	opInfoAssistviaReportingObject

Privilege	Description	Subsystems	Privilege ID
Open Items	User can open items (also requires privilege for the tool used to create the item).	WFC, EDA, WEB	opOpen
Save OPS Portlet Customization	User can save own customized view of an Open Portal Services portlet.	Session	opCustomizeOPS
Share Private Library Content	User can share own library content and watch list reports with assigned users.	WFC	opShareLibraryReport
Share Private Resources	User can share private resources with assigned users.	WFC	opShareBasic
Share Private Resources with Specific Users	User can share private resources with subset of assigned users.	WFC	opShareAdvanced
Upload Data	User can upload supported data file types to the Reporting Server.	Session, WFC, EDA	opUploadDataFile
Upload Documents	User can upload supported document file types to the repository.	Session, WFC, FILE	opUploadDocument
Upload Images	User can upload supported image file types to the repository.	Session, WFC, EDA	opUploadImage
Web Services	User can use TIBCO WebFOCUS Web Services.	Session	opWebServices

## Scheduling and Distribution

The following privileges can be assigned to users, developers, and administrators so they can create schedules that distribute reports with ReportCaster.

Privilege	Description	Subsystem	Privilege ID
Access Blackout Periods	User can view periods not available for report scheduling.	Session	opRCBlackoutDatesTool
Access Job Logs	User can view logs associated with authorized ReportCaster jobs.	Session	opRCJobLogsTool
Access Job Status	User can view status of authorized ReportCaster jobs.	Session	opRCJobStatusTool
Assign Credentials for Schedules	User can manage credentials used by schedules to connect to Reporting Servers, FTP servers, and web servers.	Session	opRCExecutionId
Create Access List	User can create an access list that limits which authorized users can view report library output.	Session, WFC	opSchedAccessList
Create Distribution List	User can create and access distribution lists associated with a schedule.	Session, WFC	opSchedDistributionList
Create Library Item	User can create Library item.	WFC	opCreateLibraryItem
Display ReportCaster Explorer	Displays the <i>ReportCaster Explorer</i> option in the Tools menu.	Session, WFC	opRCExplorer
Distribute to Email	User can schedule jobs that distribute output using email.	Session, WFC	opDistributeEmail
Distribute to File System	User can schedule jobs that distribute output to the File System.	Session, WFC	opDistributeFileSystem
Distribute to FTP	User can schedule jobs that distribute output to an FTP server.	Session, WFC	opDistributeFTP

Privilege	Description	Subsystem	Privilege ID
Distribute to Library	User can schedule jobs that distribute output to the report library.	Session, WFC	opDistributeLibrary
Distribute to Printer	User can schedule jobs that distribute output to a printer.	Session, WFC	opDistributePrinter
Distribute to Repository	User can distribute output to the repository.	Session, WFC	opDistributeMR
ReportCaster Advanced UI	Displays the <i>Schedule</i> option in the folder shortcut menu, so the user can create multi-task schedules.	Session, WFC, EDA	opScheduleAdvancedTool
Schedule Files	User can schedule the distribution of files from the ReportCaster Distribution Server operating system.	Session, WFC	opScheduleTaskFile
Schedule FTP Resources	User can schedule the distribution of files from an FTP server.	Session, WFC	opScheduleTaskFTP
Schedule HTTP Requests	User can schedule the distribution of HTTP responses obtained from a web server.	Session, WFC	opScheduleTaskURL
Schedule Other Schedules	User can schedule other schedules.	Session, WFC	opScheduleTaskSchedule
Schedule MR Procedures	User can schedule Managed Reporting procedures.	Session, WFC	opScheduleTaskMR
Schedule Reporting Server Procedures	User can schedule procedures located in a Reporting Server application folder.	Session, WFC	opScheduleTaskWFRS

## Application Development

The following privileges can be assigned to developers so they can create complete WebFOCUS applications using only web-based tools. To enable access to the full set of WebFOCUS application development capabilities, you should also assign the privileges in the Desktop Development category to your development team.

Privilege	Description	Subsystems	Privilege ID
Copy and Update Paths	TIBCO WebFOCUS adjusts path references for copied items.  <b>Note:</b> This privilege is available as a Technical Preview feature as of Release 8206.06.	WFC	opCopySpecial
Create Folders	User can create folders.	WFC, EDA, WEB	opCreateFL
Create Items	User can create items.	WFC, BIP, EDA, WEB	opCreateItem
Create Metadata	User can access the Reporting Server Console Metadata Wizard from the Metadata menu on a folder.	Session, WFC, EDA	opMetadata
Create Portal	User can create portals.	Session, WFC, BIP	opCreatePortal
Create Reporting Objects	User can create Reporting Objects in a folder.	WFC	opReportingObject
Delete Resources	User can delete resources.	*	opDelete
Edit Items	User can edit resource content.	*	opWrite
Edit OPS Portlets	User can change what is displayed in an Open Portal Services portlet.	Session	opEditOPS

Privilege	Description	Subsystems	Privilege ID
Edit Resource Names	User can change the IBFS names of resources.	WFC, BIP, EDA	opRename
Edit Resource Properties	User can change folder and item properties.	WFC, BIP	opUpdProps
Portal Designer	User can use Portal Designer.	Session, WFC, BIP	opEditPortal
Portal Page Designer	User can use the Portal Page Designer to create and edit portal pages.	Session, WFC, BIP	opPageDesigner
Reporting Server Console	User can access the Reporting Server Console and access features authorized to Reporting Server role.	EDA	opServerConsole
Resource Export	User can export resources and change packages.	*	opExport
Resource Export Download	User can download Change Management Zip file.	*	opDownloadCM
Resource Publish	User can publish private resources so their access is governed by security policy.	WFC, BIP	opPublish
Resource Unpublish	User can make published resources private.	WFC, BIP	opMakePrivate
Resource Text Editor	User can change item contents with the text editor.	Session	opEditor
Run with SQL Traces	User can run procedures to obtain SQL Traces.	WFC	opRunSQLTrace
Session Traces	User can enable and view their own session traces.	Session	opDevTraces



Privilege	Description	Subsystems	Privilege ID
Validate Portal	User can validate portals to ensure their content is available to users.	WFC, BIP	opValidatePortal
View Rules on a Resource	User can view rules on resources.	*	opViewRulesOn

## Desktop Development

The following privileges make it possible for application developers to use WebFOCUS desktop products. These privileges must be assigned along with those in the Application Development, Advanced Reporting, and Basic Reporting categories to enable the full set of development capabilities.

Privilege	Description	Subsystems	Privilege ID
Desktop Alert	User can create alerts that conditionally run procedures.	WFC	opDTAlert
Desktop Allocation	User can assign logical names to physical files.	WFC	opDTAllocation
Desktop Chart	User can create charts from the Desktop Product.	WFC	opDTChart
Desktop Connect	User can connect the Desktop Product to TIBCO WebFOCUS.	Session	opDTConnect
Desktop Define	User can create virtual defined fields.	WFC	opDTDefine
Desktop Define Function	User can create Define functions.	WFC	opDTDefineFunction
Desktop Dialog Manager	User can control the flow of procedures using scripting.	WFC	opDTDialogManager

Privilege	Description	Subsystems	Privilege ID
Desktop Document	User can create compound documents consisting of multiple reports, charts, and images.	WFC	opDTDocumentCanvas
Desktop Editor	User can edit reports, graphs, and other objects with the Desktop text editor.	WFC	opDTEditor
Desktop Engine Facility	User can create connection commands to access data sources.	WFC	opDTEngine
Desktop Execute	User can call procedures from within other procedures.	WFC	opDTExecute
Desktop File View Panel	User can use the File View panel in Application Studio.	WFC	opDTFileViewPanel
Desktop HTML	User can create HTML pages that incorporate forms, reports, charts, maps, and other objects.	WFC	opDTHTMLCanvas
Desktop HTMLFORM	User can create - HTMLFORM commands within procedures.	WFC	opDTHTMLForm
Desktop Impact Analysis	User can analyze the use of metadata across applications.	WFC	opDTImpactAnalysis
Desktop Include	User can reference reusable code excerpts from other procedures.	WFC	opDTInclude
Desktop Join	User can join data sources.	WFC	opDTJoin
Desktop Match	User can merge data sources with Match.	WFC	opDTMatch

Privilege	Description	Subsystems	Privilege ID
Desktop OLAP Dimension Builder	User can create temporary hierarchies and dimensions within procedures.	WFC	opDTOlap
Desktop Procedure Viewer	User can view procedures with the Desktop Product Procedure Viewer.	WFC	opDTProcedureViewer
Desktop Report	User can create reports from the Desktop product.	WFC	opDTReport
Desktop RSTAT Facility	User can create predictive and scoring applications.	WFC	opDTRstat
Desktop Set	User can customize product behavior with environment settings.	WFC	opDTSet
Desktop Source Control	Enables Desktop product integration with supported version control systems.	Session, WFC	opDTSourceControl
Desktop SQL Editor	User can embed SQL code within procedures.	WFC	opDTSQLEditor
Desktop SQL Report Wizard	User can create procedures with SQL Report Wizard.	WFC	opDTSQLReport
Desktop Use	User can specify the name and location of FOCUS data sources.	WFC	opDTUse

## Group Administration

The following privileges can be assigned to department or tenant group administrators so that they can manage their users and the content created by their users.

Privilege	Description	Subsystems	Privilege ID
Access Roles	User can view these roles in the security rules dialog.	ROLES	opViewPermSet
Access Users	User can view these users in lists.	GROUPS	opListUser
Assign Ownership	User can change the owner of a resource to assigned users and groups.	WFC, BIP	opUpdateOwnership
Assign Ownership to Groups	User can assign ownership of a resource to these groups.	GROUPS	opSetGroupOwner
Assign Ownership to Users	User can assign ownership of a resource to users in these groups.	GROUPS	opSetUserOwner
Content Sharing Scope	User can share resources with users in these groups.	GROUPS	opShareWith
Group Creation	User can create groups within these groups.	GROUPS	opCreateGroup
Group Deletion	User can delete groups within these groups.	GROUPS	opDeleteGroup
Group Property Access	User can view the properties of these groups.	GROUPS	opViewGroup
Group Property Management	User can update the properties of these groups.	GROUPS	opUpdateGroup
Group Rename	User can rename groups within these groups.	GROUPS	opRenameGroup

Privilege	Description	Subsystems	Privilege ID
Manage Comments	User can manage comments on content.	Session,WFC	opManageComments
Manage General Access	User can permit everyone basic access on these resources.	Session	opGeneralAccess
Manage Group Membership	User can manage the membership of these groups.	GROUPS	opAssignUsersTo
Manage Private Resources	User can manage the private resources of users in these groups - enables Manage Private Resources in the Administration menu.	GROUPS	opManagePrivateResources
Manage ReportCaster Blackout Periods	User can manage ReportCaster blackout periods for schedules in these groups.	GROUPS	opSetBlackoutDates
Manage Rules for a Group	User can create security rules for these groups.	GROUPS	opUseGroupInRules
Manage Rules for a User	User can create security rules for these users.	GROUPS	opUseUserInRules
Manage Rules on Resources	User can manage rules on these resources.	*	opManageRulesOn
ReportCaster Administration Scope	User can manage ReportCaster resources owned by users in these groups.	GROUPS	opRCGroupAdmin
Security Center	Displays the <i>Security Center</i> option in the Administration menu, so users can manage assigned users, groups, and roles.	Session	opManageSecurity

Privilege	Description	Subsystems	Privilege ID
Security Center Scope	User can add these users to assigned groups.	GROUPS	opAssignUsersFrom
Use Roles in a Rule	User can create security rules with these roles.	ROLES	opUsePermSetInRules
User Account Creation	User can create users within these groups.	USERS, GROUPS	opCreateUser
User Account Deletion	User can delete users within these groups.	USERS, GROUPS	opDeleteUser
User Account Password Management	User can reset passwords for these users.	USERS, GROUPS	opSetPassword
User Account Property Access	User can view account properties of these users.	USERS, GROUPS	opViewUser
User Account Property Management	User can update account properties of these users.	USERS, GROUPS	opUpdateUser

## Administration

The following privileges are generally assigned only to WebFOCUS administrators.

Privilege	Description	Subsystems	Privilege ID
Allow My Content Folders	TIBCO WebFOCUS displays the Auto Create My Content Folders property on folders.	WFC	opAutocreateMyFolders
Create Roles	User can create roles.	ROLES	opCreatePermSet
Delete Roles	User can delete roles.	ROLES	opDeletePermSet
Display Administration Console	TIBCO WebFOCUS displays the <i>Administration Console</i> option in the Administration menu.	Session	opWFAdminConsole

Privilege	Description	Subsystems	Privilege ID
Display Magnify Console	TIBCO WebFOCUS displays the <i>Magnify Console</i> option in the Administration menu so users can configure the search system.	Session	opMagnifyConsole
Group Mapping	User can map TIBCO WebFOCUS groups to external authorization sources.	GROUPS	opExternalGroupMapping
Manage ReportCaster Configuration	TIBCO WebFOCUS displays the <i>ReportCaster Configuration</i> option in the Administration menu.	Session	opRCConfiguration
Manage ReportCaster Global Settings	User can perform global updates to ReportCaster content.	Session	opRCGlobalUpdate
Manage ReportCaster Library Report Deletion	User can run the Report Library deletion utility.	Session	opRCExpLibraryDelete
Manage ReportCaster Log Purge	User can run the ReportCaster Log purge utility.	Session	opRCPurgeJobLogs
Manage ReportCaster Schedule Deletion	User can run the ReportCaster Schedule deletion utility.	Session	opRCSchedDelete
Manage ReportCaster Watch List Subscription	User can unsubscribe other uses from Library Reports.	Session	opRCUnsubscribe
Manage Reporting Server Properties	User can update the Reporting Server properties on a resource.	WFC	opRepSrvProps
ReportCaster Server Administration	User can manage ReportCaster Distribution Servers.	Session	opRCServerManagement

Privilege	Description	Subsystems	Privilege ID
Resource Import	User can import resources and change packages.	*	opImport
Resource Import Upload	User can upload Change Management Zip file.	*	opUploadCM
Resource Templates	User can use resource templates from context menu in top-level folders.	Session,WFC, FILE	opUseTemplate
Update Roles	User can change roles.	ROLES	opUpdatePermSet
System Configuration	User can change the WebFOCUS system configuration.	Session	opWFAdminConfiguration
System Tracing	User can create and view WebFOCUS system Traces.	Session	opWFAdminTraces
Toggle Repository View	User can switch the resource tree to full IBFS view.	Session	opToggleTree



## Providing Data Source Security: DBA

---

As Database Administrator, you can use DBA security features to provide security for any FOCUSdata source. You can use these security features to limit the number of records or reads a user can request in a report.

You can also use DBA security features to provide security for non-FOCUS® data sources. Note that DBA security cannot protect a data source from non-WebFOCUS access.

**Note:** All references to FOCUS data sources also apply to XFOCUS data sources.

### In this appendix:

- ❑ [Introduction to Data Source Security](#)
  - ❑ [Implementing Data Source Security](#)
  - ❑ [Specifying an Access Type: The ACCESS Attribute](#)
  - ❑ [Limiting Data Source Access: The RESTRICT Attribute](#)
  - ❑ [Controlling the Source of Access Restrictions in a Multi-file Structure](#)
  - ❑ [Adding DBA Restrictions to the Join Condition](#)
  - ❑ [Placing Security Information in a Central Master File](#)
  - ❑ [Summary of Security Attributes](#)
  - ❑ [Hiding Restriction Rules: The ENCRYPT Command](#)
  - ❑ [FOCEXEC Security](#)
- 

## Introduction to Data Source Security

The DBA facility provides a number of security options:

- ❑ You can limit the user who have access to a given data source using the USER attribute discussed in [Identifying Users With Access Rights: The USER Attribute](#) on page 657.
- ❑ You can restrict a user access rights to read, write, or update only using the ACCESS attribute discussed in [Specifying an Access Type: The ACCESS Attribute](#) on page 662.
- ❑ You can restrict a user access to certain fields or segments using the RESTRICT attribute discussed in [Limiting Data Source Access: The RESTRICT Attribute](#) on page 665.

- ❑ You can ensure that only records that pass a validation test are retrieved using the RESTRICT attribute discussed in [Limiting Data Source Access: The RESTRICT Attribute](#) on page 665.
- ❑ You can limit the values a user can read or write to the data source or you can limit which values a user can alter using the RESTRICT attribute discussed in [Limiting Data Source Access: The RESTRICT Attribute](#) on page 665.
- ❑ You can control the source of access restrictions in a multi-file structure using the SET DBASOURCE command discussed in [Controlling the Source of Access Restrictions in a Multi-file Structure](#) on page 672.
- ❑ You can point to passwords and restrictions stored in another Master File with the DBAFILE attribute discussed in [Placing Security Information in a Central Master File](#) on page 676.
- ❑ You can use the WebFOCUS DBA exit routine to allow an external security system to set the WebFOCUS password. For more information, see the *TIBCO WebFOCUS® Security and Administration* manual.
- ❑ You can place security on FOCEXECs, as discussed in [FOCEXEC Security](#) on page 686.

## Implementing Data Source Security

You provide WebFOCUS security on a file-by-file basis. Implementing DBA security features is a straightforward process in which you specify:

- ❑ The names or passwords of WebFOCUS users granted access to a data source.
- ❑ The type of access the user is granted.
- ❑ The segments, fields, or ranges of data values to which the user access is restricted.

The declarations (called security declarations) follow the END command in a Master File and tell WebFOCUS that security is needed for the data source and what type of security is needed. Each security declaration consists of one or several of the following attributes:

- ❑ The DBA attribute gives the name or password of the Database Administrator for the data source. The Database Administrator has unlimited access to the data source and its Master File.
- ❑ The USER attribute identifies a user as a legitimate user of the data source. Only users whose name or password is specified in the Master File of a FOCUS data source with security placed on it have access to that data source.

- ❑ The ACCESS attribute defines the type of access a given user has. The four types of access available are:

RW, which allows a user to both read and write to a data source.

R, which allows a user only to read data in a data source.

W, which allows a user to only write new segment instances to a data source.

U, which allows a user only to update records in a data source.

- ❑ The RESTRICT attribute specifies certain segments or fields to which the user is not granted access. It can also be used to restrict the data values a user can see or perform transactions on.
- ❑ The NAME and VALUE attributes are part of the RESTRICT declaration.

Describe your data source security by specifying values for these attributes in a comma-delimited format, just as you specify any other attribute in the Master File.

The word END on a line by itself in the Master File terminates the segment and field attributes and indicates that the access limits follow. If you place the word END in a Master File, it must be followed by at least a DBA attribute.

### **Example:** Implementing Data Source Security in a Master File

The following is a Master File that uses security features:

```

FILENAME = PERS, SUFFIX = FOC,$
SEGMENT = IDSEG, SEGTYPE = S1,$
  FIELD = SSN           ,ALIAS = SSN      ,FORMAT = A9      ,,$
  FIELD = FULLNAME      ,ALIAS = FNAME    ,FORMAT = A40     ,,$
  FIELD = DIVISION      ,ALIAS = DIV      ,FORMAT = A8      ,,$
SEGMENT=COMPSEG, PARENT=IDSEG, SEGTYPE=S1,$
  FIELD = SALARY         ,ALIAS = SAL      ,FORMAT = D8      ,,$
  FIELD = DATE           ,ALIAS = DATE     ,FORMAT = YMD     ,,$
  FIELD = INCREASE       ,ALIAS = INC      ,FORMAT = D6      ,,$
END
DBA=JONES76,$
USER=TOM      ,ACCESS=RW, $
USER=BILL     ,ACCESS=R  ,RESTRICT=SEGMENT ,NAME=COMPSEG ,,$
USER=JOHN     ,ACCESS=R  ,RESTRICT=FIELD  ,NAME=SALARY  ,,$
               ,NAME=INCREASE ,,$
USER=LARRY    ,ACCESS=U  ,RESTRICT=FIELD  ,NAME=SALARY  ,,$
USER=TONY     ,ACCESS=R  ,RESTRICT=VALUE  ,NAME=IDSEG,
  VALUE=DIVISION EQ 'WEST' ,,$
USER=MARY     ,ACCESS=W  ,RESTRICT=VALUE  ,NAME=SALTEST ,
  VALUE=INCREASE+SALARY GE SALARY,$
               ,NAME=HISTTEST,
  VALUE=DIV NE ' ' AND DATE GT 0,$

```

**Reference: Special Considerations for Data Source Security**

- ❑ When using the JOIN command, it is possible to bypass the DBA information in a data source. This is a security exposure created because in a JOIN structure the DBA information is read from the host Master File. This problem is solved by using the DBAFILE feature discussed in [Placing Security Information in a Central Master File](#) on page 676. All data sources in the joined structure will get security information as coded in the DBAFILE.
- ❑ The DBA section of a Master File cannot have comments within it.

**Identifying the DBA: The DBA Attribute**

The first security attribute should be a password that identifies the Database Administrator. This password can be up to 64 characters long and is not case-sensitive. It can include special characters. If the DBA password contains blanks, it must be enclosed in single quotation marks. Since nothing else is needed, this line is terminated by the usual delimiter (,\$).

**Note:**

- ❑ Every data source having access limits must have a DBA.
- ❑ Groups of cross-referenced data sources must have the same DBA value.
- ❑ Partitioned data sources, which are read together in the USE command, must have the same DBA value.
- ❑ The Database Administrator has unlimited access to the data source and all cross-referenced data sources. Therefore, no field, segment, or value restrictions can be specified with the DBA attribute.
- ❑ You cannot encrypt and decrypt Master Files or restrict existing data sources without the DBA password.
- ❑ You should thoroughly test every security attribute before the data source is used. It is particularly important to test the VALUE limits to make sure they do not contain errors. Value tests are executed as if they were extra screening conditions or VALIDATE statements typed after each request statement. Since users are unaware of the value limits, errors caused by the value limits may confuse them.

**Example: Identifying the DBA Using the DBA Attribute**

`DBA=JONES76,$`

**Procedure: How to Change a DBA Password**

The DBA has the freedom to change any of the security attributes. If you change the DBA password in the Master File for an existing FOCUS data source, you must use the RESTRICT command to store the changed DBA password in each FOCUS data source affected by the change. Unless this is done, WebFOCUS assumes that the new description is an attempt to bypass the restriction rules. You use the following procedure for each data source affected:

1. Edit the Master File, changing the DBA value from old to new.
2. Issue the command:

```
SET PASS=old_DBA_password
```

3. Issue the command:

```
RESTRICT
mastername
END
```

4. Issue the command:

```
SET PASS=new_DBA_password
```

**Including the DBA Attribute in a HOLD File**

With the SET HOLDSTAT command, you can identify a data source containing DBA information and comments to be automatically included in HOLD and PCHOLD Master Files. For more information about the SET HOLDSTAT command, see the *Developing Reporting Applications* manual.

**Identifying Users With Access Rights: The USER Attribute**

The USER attribute is a password that identifies the users who have legitimate access to the data source. A USER attribute cannot be specified alone. It must be followed by at least one ACCESS restriction (discussed in [Specifying an Access Type: The ACCESS Attribute](#) on page 662) to specify what sort of ACCESS the user is granted.

Before using a secured data source, a user must enter the password using the SET PASS or SET USER command. If that password is not included in the Master File, the user is denied access to the data source. When the user does not have a password, or has one that is inadequate for the type of access requested, the following message appears:

```
(FOC047) THE USER DOES NOT HAVE SUFFICIENT ACCESS RIGHTS TO THE FILE:
filename
```

**Syntax:**      **How to Set the USER Attribute**

Any user whose name or password is not declared in the Master File is denied access to that data source. The syntax of the USER attribute is

```
USER = name
```

where:

*name*

Is a password of up to 64 characters for the user. The password can include special characters and is not case-sensitive. If the password contains blanks, it must be enclosed in single quotation marks.

You can specify a blank password (default value if not previously changed). Such a password does not require the user to issue a SET PASS= command. A blank password may still have access limits and is convenient when a number of users have the same access rights.

**Example:**      **Setting the USER Attribute**

```
USER=TOM, . . .
```

An example of setting a user password to blank, and access to read only follows:

```
USER= , ACCESS=R,$
```

**Non-Overridable User Passwords (SET PERMPASS)**

The PERMPASS parameter establishes a user password that remains in effect throughout a session or connection. You can issue this setting in any supported profile but is most useful when established for an individual user by setting it in a user profile. It cannot be set in an ON TABLE phrase. It is recommended that it not be set in EDASPROF because it would then apply to all users.

All security rules established in the DBA sections of existing Master Files are respected when PERMPASS is in effect. The user cannot issue the SET PASS or SET USER command to change to a user password with different security rules. Any attempt to do so generates the following message:

```
(FOC32409) A permanent PASS is in effect. Your PASS will not be honored.  
VALUE WAS NOT CHANGED
```

**Note:** Only one permanent password can be established in a session. Once it is set, it cannot be changed within the session.

**Syntax:**      **How to Set a Non-Overridable User Password**

```
SET PERMPASS=userpass
```

where:

*userpass*

Is the user password used for all access to data sources with DBA security rules established in their associated Master Files.

**Example:**      **Setting a Non-Overridable User Password**

Consider the MOVIES Master File with the following DBA rules in effect:

```
DBA=USER1,$
USER = USERR, ACCESS = R,$
USER = USERU, ACCESS = U,$
USER = USERW, ACCESS = W,$
USER = USERRW, ACCESS = RW,$
```

The following FOCEXEC sets a permanent password:

```
SET PERMPASS = USERU
TABLE FILE MOVIES
PRINT TITLE BY DIRECTOR
END
```

The user has ACCESS=U and, therefore, is not allowed to issue a table request against the file:

```
(FOC047) THE USER DOES NOT HAVE SUFFICIENT ACCESS RIGHTS TO THE FILE:
CAR
BYPASSING TO END OF COMMAND
```

The permanent password cannot be changed:

```
SET PERMPASS = USERRW
```

```
(FOC32409) A permanent PASS is in effect. Your PASS will not be honored.
VALUE WAS NOT CHANGED
```

The user password cannot be changed:

```
SET PASS = USERRW
```

```
(FOC32409) A permanent PASS is in effect. Your PASS will not be honored.
VALUE WAS NOT CHANGED
```

## Controlling Case Sensitivity of Passwords

When a DBA or user issues the SET USER, SET PERMPASS or SET PASS command, this user ID is validated before they are given access to any data source whose Master File has DBA attributes. The password is also checked when encrypting or decrypting a FOCEXEC.

The SET DBACSENSITIV command determines whether the password is converted to uppercase prior to validation.

### **Syntax:** How to Control Password Case Sensitivity

```
SET DBACSENSITIV = {ON|OFF}
```

where:

ON

Does not convert passwords to uppercase. All comparisons between the password set by the user and the password in the Master File or FOCEXEC are case-sensitive.

OFF

Converts passwords to uppercase prior to validation. All comparisons between the password set by the user and the password in the Master File or FOCEXEC are *not* case-sensitive. OFF is the default value.

### **Example:** Controlling Password Case Sensitivity

Consider the following DBA declaration added to the EMPLOYEE Master File:

```
USER = User2, ACCESS = RW,$
```

User2 wants to report from the EMPLOYEE data source and issues the following command:

```
SET USER = USER2
```

With DBACSENSITIV OFF, User2 can run the request even though the case of the password entered does not match the case of the password in the Master File.

With DBACSENSITIV ON, User2 gets the following message:

```
(FOC047) THE USER DOES NOT HAVE SUFFICIENT ACCESS RIGHTS TO THE FILE:
```

With DBACSENSITIV ON, the user must issue the following command:

```
SET USER = User2
```



## Establishing User Identity

A user must enter his or her password before using any FOCUS data source that has security specified for it. A single user may have different passwords in different files. For example, in file ONE, the rights of password BILL apply, but in file TWO, the rights of password LARRY apply. Use the SET PASS command to establish the passwords.

### **Syntax:** How to Establish User Identity

```
SET {PASS|USER} = name [[IN {file|* [NOCLEAR]]], name [IN file] ...]
```

where:

*name*

Is the user name or password. If a character used in the password has a special meaning in your operating environment (for example, as an escape character), you can issue the SET USER command in a FOCEXEC and execute the FOCEXEC to set the password. If the password contains a blank, you do not have to enclose it in single quotation marks when issuing the SET USER command.

*file*

Is the name of the Master File to which the password applies.

\*

Indicates that *name* replaces all passwords active in all files.

NOCLEAR

Provides a way to replace all passwords in the list of active passwords while retaining the list.

### **Example:** Establishing User Identity

In the following example, the password TOM is in effect for all data sources that do not have a specific password designated for them:

```
SET PASS=TOM
```

For the next example, in file ONE the password is BILL, and in file TWO the password is LARRY. No other files have passwords set for them:

```
SET PASS=BILL IN ONE, LARRY IN TWO
```

Here, all files have password SALLY except files SIX and SEVEN, which have password DAVE.

```
SET PASS=SALLY, DAVE IN SIX
SET PASS=DAVE IN SEVEN
```

The password is MARY in file FIVE and FRANK in all other files:

```
SET PASS=MARY IN FIVE,FRANK
```

A list of the files for which a user has set specific passwords is maintained. To see the list of files, issue:

```
? PASS
```

When the user sets a password IN \* (all files), the list of active passwords collapses to one entry with no associated file name. To retain the file name list, use the NOCLEAR option.

In the next example, the password KEN replaces all passwords active in all files, and the table of active passwords is folded to one entry:

```
SET PASS=KEN IN *
```

In the following, MARY replaces all passwords in the existing table of active passwords (which consists of files NINE and TEN) but FRANK is the password for all other files. The option NOCLEAR provides a shorthand way to replace all passwords in a specific list:

```
SET PASS=BILL IN NINE,TOM IN TEN  
SET PASS=MARY IN * NOCLEAR,FRANK
```

**Note:** The FIND function does not work with COMBINED data sources secured with different passwords.

Users must issue passwords using the SET PASS command during each session in which they use a secured data source. They may issue passwords at any time before using the data source and can issue a different password afterward to access another data source.

## Specifying an Access Type: The ACCESS Attribute

The ACCESS attribute specifies what sort of access a user is granted. Every security declaration, except the DBA declaration, must have a USER attribute and an ACCESS attribute.

The following is a complete security declaration, consisting of a USER attribute and an ACCESS attribute.

```
USER=TOM, ACCESS=RW,$
```

This declaration gives Tom read and write (for adding new segment instances) access to the data source.

You can assign the ACCESS attribute one of four values. These are:

ACCESS=R	Read-only
ACCESS=W	Write only
ACCESS=RW	Read the data source and write new segment instances
ACCESS=U	Update only

Access levels affect what kind of commands a user can issue. Before you decide what access levels to assign to a user, consider what commands that user will need. If a user does not have sufficient access rights to use a given command, the following message appears:

(FOC047) THE USER DOES NOT HAVE SUFFICIENT ACCESS RIGHTS TO THE FILE:  
*filename*

ACCESS levels determine what a user can do to the data source. Use the RESTRICT attribute (discussed in [Limiting Data Source Access: The RESTRICT Attribute](#) on page 665) to limit the fields, values, or segments to which a user has access. Every USER attribute must be assigned an ACCESS attribute. The RESTRICT attribute is optional. Without it, the user has unlimited access to fields and segments within the data source.

## Types of Access

The type of access granting use of various WebFOCUS commands is shown in the following table. When more than one type of access is shown, any type of access marked will allow the user at least some use of that command. Often, however, the user will be able to use the command in different ways, depending on the type of access granted.

Command	R	W	RW	U	DBA
CHECK	X	X	X	X	X
CREATE			X		X
DECRYPT					X
DEFINE	X		X		X
ENCRYPT					X

Command	R	W	RW	U	DBA
<b>MATCH</b>	X		X		X
<b>REBUILD</b>			X		X
<b>RESTRICT</b>					X
<b>TABLE</b>	X		X		X

**CHECK Command.** Users without the DBA password or read/write access are allowed limited access to the CHECK command. However, when the HOLD option is specified, the warning ACCESS LIMITED BY PASSWORD is produced, and restricted fields are propagated to the HOLD file depending on the DBA RESTRICT attribute. See [Limiting Data Source Access: The RESTRICT Attribute](#) on page 665 for more information on the RESTRICT attribute.

**CREATE Command.** Only users with the DBA password or read/write (RW) access rights can issue a CREATE command.

**DECRYPT Command.** Only users with the DBA password can issue a DECRYPT command.

**DEFINE Command.** As with all reporting commands, a user need only have an access of R (read only) to use the DEFINE command. An access of R permits the user to read records from the data source and prepare reports from them. The only users who cannot use the DEFINE command are those whose access is W (write only) or U (update only).

**ENCRYPT Command.** Only users with the DBA password can use the ENCRYPT command.

**REBUILD Command.** Only users with the DBA password or read/write (RW) access rights can issue the REBUILD command. This command is only for FOCUS data sources.

**RESTRICT Command.** Only users with the DBA password may use the RESTRICT command.

**TABLE or MATCH Command.** A user who has access of R or RW may use the TABLE command. Users with access of W or U may not.

**Reference: RESTRICT Attribute Keywords**

The RESTRICT attribute keywords affect the resulting HOLD file created by the CHECK command as follows:

**FIELD**

Fields named with the NAME parameter are not included in the HOLD file.

**SEGMENT**

The segments named with the NAME parameter are included, but fields in those segments are not.

**SAME**

The behavior is the same as for the user named in the NAME parameter.

**NOPRINT**

Fields named in the NAME or SEGNAME parameter are included since the user can reference these.

**VALUE**

Fields named in the VALUE parameter are included since the user can reference these.

If you issue the CHECK command with the PICTURE option, the RESTRICT attribute keywords affect the resulting picture as follows:

**FIELD**

Fields named with the NAME parameter are not included in the picture.

**SEGMENT**

The boxes appear for segments named with the NAME parameter, but fields in those segments do not.

**SAME**

The behavior is the same as for the user named in the NAME parameter.

**NOPRINT**

This option has no effect on the picture.

**VALUE**

This option has no effect on the picture.

**Limiting Data Source Access: The RESTRICT Attribute**

The ACCESS attribute determines what a user can do with a data source.

The optional RESTRICT attribute further restricts a user access to certain fields, values, or segments.

The RESTRICT=VALUE attribute supports those criteria that are supported by the IF phrase. The RESTRICT=VALUE\_WHERE attribute supports all criteria supported in a WHERE phrase, including comparison between fields and use of functions. The WHERE expression will be passed to a configured adapter when possible.

**Syntax:**      **How to Limit Data Source Access**

```
...RESTRICT=level, NAME={name|SYSTEM} [,VALUE=test],$,
```

or

```
...RESTRICT=VALUE_WHERE, NAME=name, VALUE=expression; ,$,
```

where:

*level*

Can be one of the following:

- ☐ **FIELD.** which specifies that the user cannot access the fields named with the NAME parameter.
- ☐ **SEGMENT.** which specifies that the user cannot access the segments named with the NAME parameter.
- ☐ **PROGRAM.** which specifies that the program named with the NAME parameter will be called whenever the user uses the data source.
- ☐ **SAME.** which specifies that the user has the same restrictions as the user named in the NAME parameter. No more than four nested SAME users are valid.
- ☐ **NOPRINT.** which specifies that the field named in the NAME or SEGMENT parameter can be mentioned in a request statement, but will not display. You can use a VALUE test to limit the restriction to values that satisfy an expression. For example, consider the following RESTRICT=NOPRINT declaration. User MARY can only display the IDs of those employees whose salaries are less than 10000.

```
USER=MARY ,ACCESS=R ,RESTRICT=NOPRINT ,NAME=EMP_ID ,  
VALUE=Curr_Sal LT 10000;,$
```

**Note:** A field with RESTRICT=NOPRINT can be referenced in a display command (verb), but not in any type of filtering command, such as IF, WHERE, FIND, LOOKUP, or VALIDATE.

*name*

Is the name of the field or segment to restrict. When used after NOPRINT, this can only be a field name. NAME=SYSTEM, which can only be used with value tests, restricts every segment in the data source, including descendant segments. Multiple fields or segments can be specified by issuing the RESTRICT attribute several times for one user.

**Note:** With value restrictions, NAME=segment restricts the named segment and any segment lower in the hierarchy, whether or not an alternate file view changes the retrieval view. This means that if a parent segment has a value restriction, and a join or alternate file view makes a child segment the new root, the value restriction on the original parent will still apply to the new root.

## VALUE

Specifies that the user can have access to only those values that meet the test described in the *test* parameter.

*test*

Is the value test that the data must meet before the user can have access to it. The test is an expression supported in an IF phrase.

## VALUE\_WHERE

Specifies that the user can have access to only those values that meet the test described in the *expression* parameter.

*expression;*

Is the value test that the data must meet before the user can have access to it. The test is an expression supported in a WHERE phrase.

**Note:** The semicolon (;) is required.

**Example: Restricting Access to Values Using VALUE\_WHERE**

Add the following DBA declarations to the end of the GGSALES Master File. These declarations give USER1 access to the West region and to products that start with the letter C:

```
END
DBA = USERD,$
USER = USER1, ACCESS = R, NAME = SALES01, RESTRICT = VALUE_WHERE,
      VALUE = REGION EQ 'West' AND PRODUCT LIKE 'C%'; , $
```

The following request sets the password to USER1 and sums dollar sales and units by REGION, CATEGORY, and PRODUCT:

```
SET USER = USER1
TABLE FILE GGSales
SUM DOLLARS UNITS
BY REGION
BY CATEGORY
BY PRODUCT
END
```

The output only displays those regions and products that satisfy the WHERE expression in the Master File:

Region	Category	Product	Dollar Sales	Unit Sales
-----	-----	-----	-----	-----
West	Coffee	Capuccino	915461	72831
	Food	Croissant	2425601	197022
	Gifts	Coffee Grinder	603436	48081
		Coffee Pot	613624	47432

If the RESTRICT=VALUE\_WHERE attribute is changed to a RESTRICT=VALUE attribute, the expression is not valid, the following message is generated, and the request does not execute:

```
(FOC002) A WORD IS NOT RECOGNIZED: LIKE 'C%'
```

**Example:**    **Limiting Data Source Access**

```
USER=BILL ,ACCESS=R ,RESTRICT=SEGMENT ,NAME=COMPSEG,$
```

**Restricting Access to a Field or a Segment**

The RESTRICT attribute identifies the segments or fields that the user will not be able to access. Anything not named in the RESTRICT attribute will be accessible.

Without the RESTRICT attribute, the user has access to the entire data source. Users may be limited to reading, writing, or updating new records, but every record in the data source is available for the operation.

**Syntax:**    **How to Restrict Access to a Field or a Segment**

```
...RESTRICT=level,    NAME=name, $
```

where:

*level*

Can be one of the following:

**FIELD** specifies that the user cannot access the fields named with the NAME parameter.



**SEGMENT** specifies that the user cannot access the segments named with the NAME parameter.

**SAME** specifies that the user has the same restrictions as the user named in the NAME parameter.

**NOPRINT** specifies that the field named in the NAME or SEGMENT parameter can be mentioned in a request statement but will not appear. When used after NOPRINT, NAME can only be a field name. A field with RESTRICT=NOPRINT can be referenced in a display command (verb), but not in any type of filtering command, such as IF, WHERE, FIND, LOOKUP, or VALIDATE.

#### *name*

Is the name of the field or segment to restrict. When used after NOPRINT, this can only be a field name.

NAME=SYSTEM, which can only be used with value tests, restricts every segment in the data source, including descendant segments. Multiple fields or segments can be specified by issuing the RESTRICT attribute several times for one user.

#### **Note:**

- ❑ If a field or segment is mentioned in the NAME attribute, it cannot be retrieved by the user. If such a field or segment is mentioned in a request statement, it will be rejected as beyond the user access rights. With NOPRINT, the field or segment can be mentioned, but the data will not appear. The data will appear as blanks for alphanumeric format or zeros for numeric fields. A field with RESTRICT=NOPRINT can be referenced in a display command (verb), but not in any type of filtering command, such as IF, WHERE, FIND, LOOKUP, or VALIDATE.

- ❑ You can restrict multiple fields or segments by providing multiple RESTRICT statements. For example, to restrict Harry from using both field A and segment B, you issue the following access limits:

```
USER=HARRY, ACCESS=R, RESTRICT=FIELD, NAME=A,$
    RESTRICT=SEGMENT, NAME=B,$
```

- ❑ You can restrict as many segments and fields as you like.
- ❑ Using RESTRICT=SAME is a convenient way to reuse a common set of restrictions for more than one password. If you specify RESTRICT=SAME and provide a user name or password as it is specified in the USER attribute for the NAME value, the new user will be subject to the same restrictions as the one named in the NAME attribute. You can then add additional restrictions, as they are needed.

**Example: Restricting Access to a Segment**

In the following example, Bill has read-only access to everything in the data source except the COMPSEG segment:

```
USER=BILL ,ACCESS=R ,RESTRICT=SEGMENT ,NAME=COMPSEG,$
```

**Example: Reusing a Common Set of Access Restrictions**

In the following example, both Sally and Harry have the same access privileges as BILL. In addition, Sally is not allowed to read the SALARY field.

```
USER=BILL, ACCESS=R, RESTRICT=VALUE, NAME=IDSEG,  
    VALUE=DIVISION EQ 'WEST',$  
USER=SALLY, ACCESS=R, RESTRICT=SAME, NAME=BILL,$  
    RESTRICT=FIELD, NAME=SALARY,$  
USER=HARRY, ACCESS=R, RESTRICT=SAME, NAME=BILL,$
```

**Note:** A restriction on a segment also affects access to its descendants.

**Restricting Access to a Value**

You can also restrict the values to which a user has access by providing a test condition in your RESTRICT attribute. The user is restricted to using only those values that satisfy the test condition.

You can restrict values in one of two ways: by restricting the values the user can read from the data source, or restricting what the user can write to a data source. These restrictions are two separate functions: one does not imply the other. You use the ACCESS attribute to specify whether the values the user reads or the values the user writes are restricted.

You restrict the values a user can read by setting ACCESS=R and RESTRICT=VALUE. This type of restriction prevents the user from seeing any data values other than those that meet the test condition provided in the RESTRICT attribute. A RESTRICT attribute with ACCESS=R functions as an involuntary IF statement in a report request. Therefore, the syntax for ACCESS=R value restrictions must follow the rules for an IF test in a report request.

**Note:** RESTRICT=VALUE is not supported in Maintain Data.

**Syntax:**      **How to Restrict Values a User Can Read**

```
...ACCESS=R, RESTRICT=VALUE, NAME=name, VALUE=test,$
```

where:

*name*

Is the name of the segment which, if referenced, activates the test. To specify all segments in the data source, specify NAME=SYSTEM.

*test*

Is the test being performed.

**Example:**      **Restricting Values a User Can Read**

```
USER=TONY, ACCESS=R, RESTRICT=VALUE, NAME=IDSEG,
VALUE=DIVISION EQ 'WEST', $
```

With this restriction, Tony can only see records from the western division.

You type the test expression after VALUE=. The syntax of the test condition is the same as that used by the TABLE command to screen records, except the word IF does not precede the phrase. (Screening conditions in the TABLE command are discussed in the *Creating Reports With TIBCO WebFOCUS® Language* manual.) Should several fields have tests performed on them, separate VALUE attributes must be provided. Each test must name the segment to which it applies. For example:

```
USER=DICK, ACCESS=R, RESTRICT=VALUE, NAME=IDSEG,
VALUE=DIVISION EQ 'EAST' OR 'WEST', $
NAME=IDSEG,
VALUE=SALARY LE 10000, $
```

If a single test condition exceeds the allowed length of a line, it can be provided in sections. Each section must start with the attribute VALUE= and end with the terminator (,\$). For example:

```
USER=SAM, ACCESS=R, RESTRICT=VALUE, NAME=IDSEG,
VALUE=DIVISION EQ 'EAST' OR 'WEST', $
VALUE=OR 'NORTH' OR 'SOUTH', $
```

**Note:** The second and subsequent lines of a value restriction must begin with the keyword OR.

You can apply the test conditions to the parent segments of the data segments on which the tests are applicable. Consider the following example:

```
USER=DICK, ACCESS=R, RESTRICT=VALUE, NAME=IDSEG,  
  VALUE=DIVISION EQ 'EAST' OR 'WEST', $  
  NAME=IDSEG,  
  VALUE=SALARY LE 10000, $
```

The field named SALARY is actually part of a segment named COMPSEG. Since the test is specified with NAME=IDSEG, the test is made effective for requests on its parent, IDSEG. In this case, the request PRINT FULLNAME would only print the full names of people who meet this test, that is, whose salary is less than or equal to \$10,000, even though the test is performed on a field that is part of a descendant segment of IDSEG. If, however, the test was made effective on COMPSEG, that is, NAME=COMPSEG, then the full name of everyone in the data source could be retrieved, but with the salary information of only those meeting the test condition.

### Restricting Both Read and Write Values

In many cases, it will prove useful to issue both ACCESS=W (for data maintenance) and ACCESS=R (for TABLE) value restrictions for a user. This will both limit the values a user can write to the data source and limit the data values that the user can actually see. You do this by issuing a RESTRICT=VALUE attribute with ACCESS=R to prohibit the user from seeing any values other than those specified in the test condition. You then issue a RESTRICT=VALUE attribute with ACCESS=W that specifies the write restrictions placed on the user. You cannot use ACCESS=RW to do this.

**Note:** Write restrictions apply to data maintenance facilities not discussed in this manual. For more information, see the Maintain Data documentation.

## Controlling the Source of Access Restrictions in a Multi-file Structure

The DBASOURCE parameter determines which security attributes are used to grant access to multi-file structures. By default, access restrictions are based on the host file in a JOIN structure or the last file in a COMBINE structure. If you set the DBASOURCE parameter to ALL, access restrictions from all files in a JOIN or COMBINE structure will be enforced.

**Note:** You can also create and implement a DBAFILE to contain and enforce the access restrictions from all files in a JOIN or COMBINE structure. For information about using a central Master File to contain access restrictions, see [Placing Security Information in a Central Master File](#) on page 676.

The SET DBASOURCE command can only be issued one time in a session or connection. Any attempt to issue the command additional times will be ignored. If the value is set in a profile, no user can change it at any point in the session.

When DBASOURCE=ALL:

- ❑ In a TABLE request against a JOIN structure, access to a cross-reference file or segment is allowed only if the user has at least read access to each file in the structure.
- ❑ In a MODIFY COMBINE structure, the user must have a minimum of READ access to all files in the structure. The user requires WRITE, UPDATE, or READ/WRITE access to a file in the structure when an INCLUDE, DELETE, or UPDATE request is issued against that file.

When DBASOURCE=HOST:

- ❑ In a TABLE request, the user needs read access to the host file in the JOIN structure. All security limitations come from the host file. Note that you can create and activate a DBAFILE in order to enforce security restrictions from all files in the structure.
- ❑ In a MODIFY procedure, the user needs write access to the last file in the COMBINE structure. All security limitations come from the restrictions in the last file in the structure. Note that you can create and activate a DBAFILE in order to enforce security restrictions from all files in the structure.

### **Syntax:**      **How to Control Enforcement of Access Restrictions in a JOIN or COMBINE Structure**

```
SET DBASOURCE = {HOST|ALL}
```

where:

#### HOST

Enforces access restrictions only from the host file in a JOIN structure or the last file in a COMBINE structure unless a DBAFILE is used to enforce access restrictions to other files in the structure. HOST is the default value.

#### ALL

Requires the user to have read access to every file in a JOIN or COMBINE structure. The user needs W, U, or RW access to a file in a COMBINE structure when an INCLUDE, UPDATE, or DELETE command is issued against that file.

### **Reference:**      **Usage Notes for SET DBASOURCE**

- ❑ All files in the JOIN or COMBINE structure must have the same DBA password. If the DBA attributes are not the same, there will be no way to access the structure.

- ❑ If the SET DBASOURCE command is issued more than once in a session, the following message displays and the value is not changed:

```
(FOC32575) DBASOURCE  CANNOT BE RESET  
VALUE WAS NOT CHANGED
```

**Example: Controlling Access Restrictions in a JOIN**

The following request joins the TRAINING data source to the EMPDATA and COURSE data sources and then issues a request against the joined structure:

```
JOIN CLEAR *  
JOIN COURSECODE IN TRAINING TO COURSECODE IN COURSE AS J1  
JOIN PIN IN TRAINING TO PIN IN EMPDATA AS J2  
TABLE FILE TRAINING  
PRINT COURSECODE AS 'CODE' CTITLE  
      LOCATION AS 'LOC'  
BY LASTNAME  
WHERE COURSECODE NE ' ' '  
WHERE LOCATION EQ 'CA' OR LOCATION LIKE 'N%'  
END
```

When the Master Files do not have DBA attributes, the output is:

LASTNAME	CODE	CTITLE	LOC
-----	----	-----	---
ADAMS	EDP750	STRATEGIC MARKETING PLANNING	NJ
CASTALANETTA	EDP130	STRUCTURED SYS ANALYSIS WKSHP	NY
	AMA130	HOW TO WRITE USERS MANUAL	CA
CHISOLM	EDP690	APPLIED METHODS IN MKTG RESEARCH	NJ
FERNSTEIN	MC90	MANAGING DISTRIBUTOR SALE NETWORK	NY
GORDON	SFC280	FUND OF ACCTG FOR SECRETARIES	NY
LASTRA	MC90	MANAGING DISTRIBUTOR SALE NETWORK	NY
MARTIN	EDP130	STRUCTURED SYS ANALYSIS WKSHP	CA
MEDINA	EDP690	APPLIED METHODS IN MKTG RESEARCH	NJ
OLSON	PU168	FUNDAMNETALS OF MKTG COMMUNICATIONS	NY
RUSSO	PU168	FUNDAMNETALS OF MKTG COMMUNICATIONS	NY
SO	BIT420	EXECUTIVE COMMUNICATION	CA
WANG	PU440	GAINING COMPETITIVE ADVANTAGE	NY
WHITE	BIT420	EXECUTIVE COMMUNICATION	CA

Now, add the following DBA attributes to the bottom of the TRAINING Master File:

```
END  
DBA = DBA1,$  
USER = TUSER, ACCESS =R,$
```

Running the same request produces the following message:

```
(FOC047) THE USER DOES NOT HAVE SUFFICIENT ACCESS RIGHTS TO THE FILE:  
TRAINING  
BYPASSING TO END OF COMMAND
```

Now, issue the following SET PASS command:

```
SET PASS = TUSER
```

Add the following DBA attributes to the bottom of the COURSE Master File:

```
END
DBA = DBA1,$
USER = CUSER, ACCESS = R,$
```

Add the following DBA attributes to the bottom of the EMPDATA Master File:

```
END
DBA = DBA1,$
USER = EUSER, ACCESS = R,$
```

Note that the DBA attribute has the same value in all of the Master Files.

Now, run the request again. There will be no security violation, and the report output will be generated. Since the DBASOURCE parameter is set to HOST (the default), you can run the request using a password that is valid only in the host file.

Now, set the DBASOURCE parameter to ALL:

```
SET DBASOURCE = ALL
SET PASS = TUSER
```

Running the request produces the following message because TUSER is not a valid user for the COURSE data source:

```
(FOC052) THE USER DOES NOT HAVE ACCESS TO THE FIELD: CTITLE
```

Now, issue the following SET PASS command that sets a valid password for each file in the structure:

```
SET PASS = TUSER IN TRAINING, CUSER IN COURSE, EUSER IN EMPDATA
```

You can now run the request and generate the report output.

Once SET DBASOURCE command has been issued, its value cannot be changed. The following SET command attempts to change the value to HOST, but the query command output shows that it was not changed:

```
> > set dbasource = host
(FOC32575) DBASOURCE CANNOT BE RESET
VALUE WAS NOT CHANGED
```

## Adding DBA Restrictions to the Join Condition

When DBA restrictions are applied to a request on a multi-segment structure, by default, the restrictions are added as WHERE conditions in the report request. When the DBAJJOIN parameter is set ON, DBA restrictions are treated as internal to the file or segment for which they are specified, and are added to the join syntax.

This difference is important when the file or segment being restricted has a parent in the structure and the join is an outer or unique join.

When restrictions are treated as report filters, lower-level segment instances that do not satisfy them are omitted from the report output, along with their host segments. Since host segments are omitted, the output does not reflect a true outer or unique join.

When the restrictions are treated as join conditions, lower-level values from segment instances that do not satisfy them are displayed as missing values, and the report output displays all host rows.

For more information, see the *Creating Reports With TIBCO WebFOCUS® Language* manual.

## Placing Security Information in a Central Master File

The DBAFILE attribute enables you to place all passwords and restrictions for multiple Master Files in one central file. Each individual Master File points to this central control file. Groups of Master Files with the same DBA password may share a common DBAFILE which itself has the same DBA password.

There are several benefits to this technique, including:

- ❑ Passwords only have to be stored once when they are applicable to a group of data sources, simplifying password administration.
- ❑ Data sources with different user passwords can be JOINed or COMBINED. In addition, individual DBA information remains in effect for each data source in a JOIN or COMBINE.

The central DBAFILE is a standard Master File. Other Master Files can use the password and security restrictions listed in the central file by specifying its file name with the DBAFILE attribute.



**Note:**

- ❑ All Master Files that specify the same DBAFILE have the same DBA password.
- ❑ The central DBAFILE, like any Master File, must contain at least one segment declaration and one field declaration before the END statement that signifies the presence of DBA information. Even if a required attribute is not assigned a specific value, it must be represented by a comma. The DBA password in the DBAFILE is the same as the password in all the Master Files that refer to it. This prevents individuals from substituting their own security. All Master Files should be encrypted.
- ❑ The DBAFILE may contain a list of passwords and restrictions following the DBA password. These passwords apply to all data sources that reference this DBAFILE. In the example in [Placing Security Attributes in a Central Master File](#) on page 678, PASS=BILL, with ACCESS=R (read only), applies to all data sources that contain the attribute DBAFILE=FOUR.
- ❑ After the common passwords, the DBAFILE may specify data source-specific passwords and additions to general passwords. You implement this feature by including FILENAME attributes in the DBA section of the DBAFILE (for example, FILENAME=TWO). See [File Naming Requirements for DBAFILE](#) on page 681 for additional information about the FILENAME attribute.
- ❑ Data source-specific restrictions override general restrictions for the specified data source. In the case of a conflict, passwords in the FILENAME section take precedence. For example, a DBAFILE might contain ACCESS=RW in the common section, but specify ACCESS=R for the same password by including a FILENAME section for a particular data source.
- ❑ Value restrictions accumulate. All value restrictions must be satisfied before retrieval. In the preceding example, note the two occurrences of PASS=JOE. JOE is a common password for all data sources, but in FILENAME=THREE it carries an extra restriction, RESTRICT=..., which applies only to data source THREE.

**Syntax:****How to Place Security Attributes in a Central Master File**

```
END
DBA=dbaname, DBAFILE=filename , $
```

where:

*dbaname*

Is the same as the dbaname in the central file.

*filename*

Is the name of the central file.

You can specify passwords and restrictions in a DBAFILE that apply to every Master File that points to that DBAFILE. You can also include passwords and restrictions for specific Master Files by including FILENAME attributes in the DBAFILE.

### **Example:** Placing Security Attributes in a Central Master File

The following example shows a group of Master Files that share a common DBAFILE named FOUR:

```
ONE MASTER
FILENAME=ONE
.
.
END
DBA=ABC, DBAFILE=FOUR,$

TWO MASTER
FILENAME=TWO
.
.
END
DBA=ABC, DBAFILE=FOUR,$

THREE MASTER
FILENAME=THREE
.
.
END
DBA=ABC,
DBAFILE=FOUR,$

FOUR MASTER
FILENAME=FOUR,$
SEGNAME=mmmmm,$
FIELDNAME=fffff,$
END
DBA=ABC,$
    PASS=BILL,ACCESS=R,$
    PASS=JOE,ACCESS=R,$
FILENAME=TWO,$
    PASS=HARRY,ACCESS=RW,$
FILENAME=THREE,$
    PASS=JOE,ACCESS=R,RESTRICT=...,$
    PASS=TOM,ACCESS=R,$
```

**Example: Using DBAFILE With a Join Structure**

The following request joins the TRAINING data source to the EMPDATA and COURSE data sources, and then issues a request against the joined structure:

```
JOIN CLEAR *
JOIN COURSECODE IN TRAINING TO COURSECODE IN COURSE AS J1
JOIN PIN IN TRAINING TO PIN IN EMPDATA AS J2
TABLE FILE TRAINING
PRINT COURSECODE AS 'CODE' CTITLE
    LOCATION AS 'LOC'
BY LASTNAME
WHERE COURSECODE NE ' '
WHERE LOCATION EQ 'CA' OR LOCATION LIKE 'N%'
END
```

When the Master Files do not have DBA attributes, the output is:

LASTNAME	CODE	CTITLE	LOC
-----	----	-----	---
ADAMS	EDP750	STRATEGIC MARKETING PLANNING	NJ
CASTALANETTA	EDP130	STRUCTURED SYS ANALYSIS WKSHP	NY
	AMA130	HOW TO WRITE USERS MANUAL	CA
CHISOLM	EDP690	APPLIED METHODS IN MKTG RESEARCH	NJ
FERNSTEIN	MC90	MANAGING DISTRIBUTOR SALE NETWORK	NY
GORDON	SFC280	FUND OF ACCTG FOR SECRETARIES	NY
LAstra	MC90	MANAGING DISTRIBUTOR SALE NETWORK	NY
MARTIN	EDP130	STRUCTURED SYS ANALYSIS WKSHP	CA
MEDINA	EDP690	APPLIED METHODS IN MKTG RESEARCH	NJ
OLSON	PU168	FUNDAMNETALS OF MKTG COMMUNICATIONS	NY
RUSSO	PU168	FUNDAMNETALS OF MKTG COMMUNICATIONS	NY
SO	BIT420	EXECUTIVE COMMUNICATION	CA
WANG	PU440	GAINING COMPETITIVE ADVANTAGE	NY
WHITE	BIT420	EXECUTIVE COMMUNICATION	CA

The EMPDATA Master File will be the central DBAFILE for the request. Add the following DBA attributes to the bottom of the EMPDATA Master File:

```
END
DBA=DBA1,$
USER = EUSER, ACCESS = R,$
FILENAME = COURSE
USER = CUSER2, ACCESS=RW,$
```

With these DBA attributes, user EUSER will have read access to all files that use EMPDATA as their DBAFILE. User CUSER2 will have read/write access to the COURSE data source.

Add the following security attributes to the bottom of the COURSE Master File. These attributes makes the EMPDATA Master File the central file that contains the security attributes to use for access to the COURSE data source and it sets the DBA attribute to the same value as the DBA attribute in the EMPDATA Master File:

```
END  
DBA = DBA1, DBAFILE=EMPDATA,$
```

Add the following security attributes to the bottom of the TRAINING Master File. These attributes makes the EMPDATA Master File the central file that contains the security attributes to use for access to the TRAINING data source and it sets the DBA attribute to the same value as the DBA attribute in the EMPDATA Master File:

```
END  
DBA = DBA1, DBAFILE=EMPDATA,$
```

Now, in order to run a request against the JOIN structure, there must be a current user password with read access in effect for each file in the JOIN. Issue the following SET PASS command and run the request:

```
SET PASS = EUSER
```

or

```
SET PASS = EUSER IN *
```

The request runs and produces output because EUSER is a valid user in each of the files in the join.

Since the EMPDATA Master File identifies CUSER2 as a valid user for the COURSE Master File, you can also run the request with the following SET PASS command:

```
SET USER = EUSER IN EMPDATA, EUSER IN TRAINING, CUSER2 IN COURSE
```

Issuing a SET PASS command that does not specify a valid password for each file in the JOIN structure produces one of the following messages, and the request does not run:

```
(FOC052) THE USER DOES NOT HAVE ACCESS TO THE FIELD: fieldname
```

```
(FOC047) THE USER DOES NOT HAVE SUFFICIENT ACCESS RIGHTS TO THE FILE:  
filename
```

## File Naming Requirements for DBAFILE

When a DBAFILE includes a FILENAME attribute for a specific Master File, the FILENAME attribute in the referencing Master File must be the same as the FILENAME attribute in the DBA section of the DBAFILE. This prevents users from renaming a Master File to a name unknown by the DBAFILE.

### *Example:* DBAFILE Naming Conventions

```
ONE MASTER
FILENAME=XONE
.
.
.
END
DBA=ABC, DBAFILE=FOUR, $

FOUR MASTER
FILENAME=XFOUR
.
.
.
END
DBA=ABC, $
.
.
.
FILENAME=XONE, $
.
.
.
```

ONE MASTER is referred to in requests as TABLE FILE ONE. However, both ONE MASTER and the DBA section of the DBAFILE, FOUR MASTER, specify FILENAME=XONE.

For security reasons, the FILENAME attribute in the Master File containing the DBAFILE information should *not* be the same as the name of that Master File. Note that in Master File FOUR, the FILENAME attribute specifies the name XFOUR.

## Connection to an Existing DBA System With DBAFILE

If there is no mention of the new attribute, DBAFILE, there will be no change in the characteristics of an existing system. In the current system, when a series of data sources is JOINed, the first data source in the list is the controlling data source. Its passwords are the only ones examined. For a COMBINE, only the last data source passwords take effect. All data sources must have the same DBA password.

In the new system, the DBA sections of all data sources in a JOIN or COMBINE are examined. If DBAFILE is included in a Master File, then its passwords and restrictions are read. To make the DBA section of a data source active in a JOIN list or COMBINE, specify DBAFILE for that data source.

After you start to use the new system, convert all of your Master Files. For Database Administrators who want to convert existing systems but do not want a separate physical DBAFILE, the DBAFILE attribute can specify the data source itself.

**Example: Connecting to an Existing DBA System With DBAFILE**

```
FILENAME=SEVEN,  
  SEGNAME=. .  
  FIELDNAME=...  
  .  
  .  
  .  
END  
DBA=ABC,DBAFILE=SEVEN,$      (OR DBAFILE= , $)  
PASS=...  
PASS=...
```

**Combining Applications With DBAFILE**

Since each data source now contributes its own restrictions, you can JOIN and COMBINE data sources that come from different applications and have different user passwords. The only requirement is a valid password for each data source. You can therefore grant access rights for one application to an application under the control of a different DBA by assigning a password in your system.

You can assign screening conditions to a data source that are automatically applied to any report request that accesses the data source. See the *Creating Reports With TIBCO WebFOCUS® Language* manual for details.

**Summary of Security Attributes**

The following is a list of all the security attributes used in WebFOCUS:

Attribute	Alias	Maximum Length	Meaning
DBA	DBA	8	Value assigned is code name of the Database Administrator (DBA) who has unrestricted access to the data source.

Attribute	Alias	Maximum Length	Meaning
USER	PASS	8	Values are arbitrary code names, identifying users for whom security restrictions will be in force.
ACCESS	ACCESS	8	Levels of access for this user. Values are:  R - read-only  W - write new segments only  RW - read and write  U - update values only
RESTRICT	RESTRICT	8	Types of restrictions to be imposed for this access level. Values are:  SEGMENT FIELD VALUE SAME  NOPRINT
NAME	NAME	66	Name of segment or field restricted or program to be called.
VALUE	VALUE	80	Test expression which must be true when RESTRICT=VALUE is the type of limit.
DBAFILE	DBAFILE	8	Names the Master File containing passwords and restrictions to use.

## Hiding Restriction Rules: The ENCRYPT Command

Since the restriction information for a FOCUS data source is stored in its Master File, you can encrypt the Master File in order to prevent users from examining the restriction rules. Only the Database Administrator can encrypt a description. You must set PASS=DBAname before you issue the ENCRYPT command. The syntax of the ENCRYPT command varies from operating system to operating system.

**Note:** The first line of a Master File that is going to be encrypted cannot be longer than 68 characters. If it is longer than 68 characters, you must break it up onto multiple lines.

### **Syntax:** How to Hide Restriction Rules: ENCRYPT Command

```
ENCRYPT FILE filename
```

where:

*filename*

Is the name of the file to be encrypted.

### **Example:** Encrypting and Decrypting a Master File

The following is an example of the complete procedure:

```
SET PASS=JONES76  
ENCRYPT FILE PERS
```

The process can be reversed in order to change the restrictions. The command to restore the description to a readable form is DECRYPT.

The DBA password must be issued with the SET command before the file can be decrypted. For example:

```
SET PASS=JONES76  
DECRYPT FILE PERS
```

## Encrypting Data

You may also use the ENCRYPT parameter within the Master File to encrypt some or all of its segments. When encrypted files are stored on the external media (disk or tape) each is secure from unauthorized examination.

Encryption takes place on the segment level. That is, the entire segment is encrypted. The request for encryption is made in the Master File by setting the attribute ENCRYPT to ON.



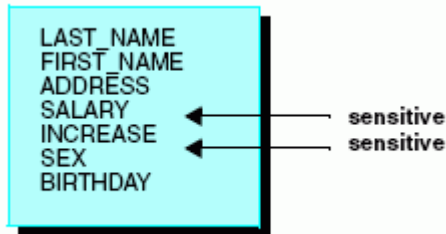
**Example: Encrypting Data**

```
SEGMENT=COMPSEG, PARENT=IDSEG, SEGTYPE=S1, ENCRYPT=ON,$
```

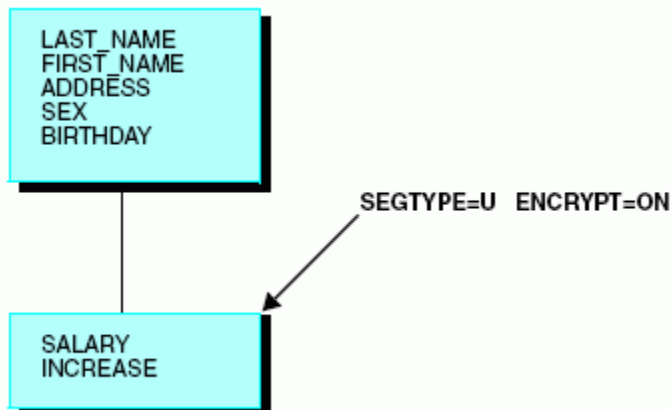
You must specify the ENCRYPT parameter before entering any data in the data source. The message NEW FILE... must appear when the encryption is first requested. Encryption cannot be requested later by a change to the Master File and cannot be removed after it has been requested or any data has been entered in the data source.

**Performance Considerations for Encrypted Data**

There is a small loss in processing efficiency when data is encrypted. Minimize this loss by grouping the sensitive data fields together on a segment and making them a separate segment of SEGTYPE=U, unique segment, beneath the original segment. For example, suppose the data items on a segment are:



They should be grouped as:



**Note:** If you change the DBA password, you must issue the RESTRICT command, as described in [How to Change a DBA Password](#) on page 657.

### Setting a Password Externally

Passwords can also be set automatically by an external security system such as RACF®, CA-ACF2®, or CA-Top Secret®. Passwords issued this way are set when WebFOCUS first enters and may be permanent (that is, not alterable by subsequent SET USER, SET PASS, or -PASS commands). Or they may be default passwords that can be subsequently overridden. The passwords may be permanent for some users, defaults for other users, and not set at all for other users.

The advantage of setting WebFOCUS passwords externally is that the password need not be known by the user, does not require prompting, and does not have to be embedded in a PROFILE FOCEXEC or an encrypted FOCEXEC.

Passwords set this way must match the passwords specified in the Master Files of the data sources being accessed.

## FOCEXEC Security

Most data security issues are best handled by WebFOCUS DBA exit routines. For more information about WebFOCUS DBA exit routines see the *TIBCO WebFOCUS® Security and Administration* manual. You can also encrypt and decrypt FOCEXECs.

### Encrypting and Decrypting a FOCEXEC

Keep the actual text of a stored FOCEXEC confidential while allowing users to execute the FOCEXEC. You do this either because there is confidential information stored in the FOCEXEC or because you do not want the FOCEXEC changed by unauthorized users. You can protect a stored FOCEXEC from unauthorized users with the ENCRYPT command.

Any user can execute an encrypted FOCEXEC, but you must decrypt the FOCEXEC to view it. Only a user with the encrypting password can decrypt the FOCEXEC.

The password selected by a user to ENCRYPT or DECRYPT a FOCEXEC is not viewable by any editor and it is unrelated to the DBA passwords of the files being used.

### **Syntax:** How to Encrypt and Decrypt a FOCEXEC

You use the following procedure to encrypt the FOCEXEC named SALERPT:

```
SET PASS = DOHIDE  
ENCRYPT FILE SALERPT FOCEXEC
```

You use the following procedure to decrypt the FOCEXEC named SALERPT:

```
SET PASS = DOHIDE  
DECRYPT FILE SALERPT FOCEXEC
```



## App Studio Custom Logon Templates

---

If you are protecting WebFOCUS with custom security, you may be able to access WebFOCUS from App Studio by using a custom logon template. Logon templates are developed by an administrator and describe certain behavior specific to the custom security solution.

The template uses XML tags to describe:

- ❑ How to locate the logon resource (which can be a servlet, JSP, ASP, or CGI that will sign the user in to the security system).
- ❑ The logon results. After a successful sign-in, the security system must return a cookie. App Studio software will then continuously forward this cookie to the site, protecting the WebFOCUS installation for the duration of its session.

An administrator with technical knowledge about the security system creates these templates, which are distributed to each developer or referenced from a shared location on the network. Developers may then select a custom logon template from the Environment Properties dialog box and use it to access the protected WebFOCUS environment.

### In this appendix:

- ❑ [How Logon Templates Work](#)
  - ❑ [Creating a Custom Template](#)
  - ❑ [Configuring App Studio to Support IBM Tivoli Access Manager WebSEAL](#)
  - ❑ [Additional WebSEAL Configuration Steps](#)
- 

## How Logon Templates Work

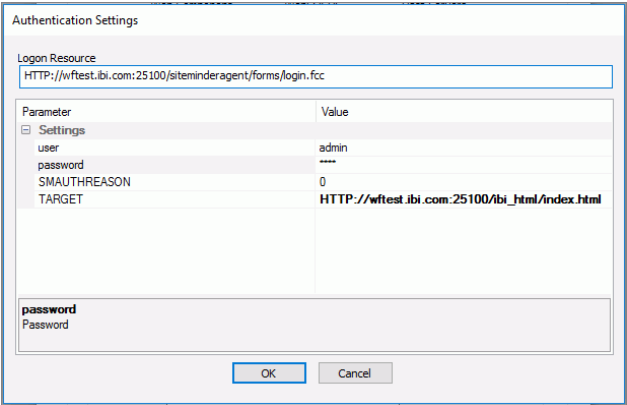
Custom logon templates are stored in a file named dssso.xml. This file is installed with the App Studio software in the `drive:\ibi\AppStudio82\bin` directory and is located using the following Windows registry key:

```
HKEY_CURRENT_USER\Software\Information Builders\  
AppStudio\82\FOCSHELL\WFSCOM
```

By default, this key points to the *drive:\ibi\AppStudio82\bin\dssso.xml* file, which contains templates for the following security providers:

- ☐ SiteMinder®.
- ☐ WebSEAL.
- ☐ Oracle Access Manager.
- ☐ Basic, IWA, and Kerberos do not use templates.

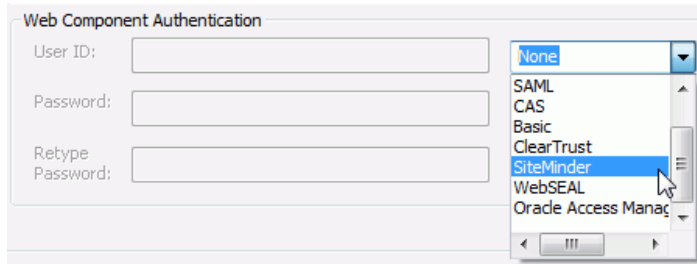
You can use drive letter mapping or the Universal Naming Convention (for example, `\\wftest\sharedfiles\dssso.xml`) to point to a shared network copy of the file.



**Procedure: How to Select the Logon Template**

1. Open WebFOCUS App Studio.
2. On the *Home* tab, in the *Utilities* group, click *Environments*.  
The Environments List dialog box opens.
3. Highlight an environment, then click *Properties*.  
The WebFOCUS Environments Properties dialog box opens.

4. In the Web Component Authentication section, choose an available template from the drop-down menu, as shown in the following image.



5. Type a user ID and password in the User ID and Password fields.

App Studio tries to locate the logon template file when it first opens. If no file is found, only None and Basic are displayed in the list. If the file is found, the logon templates in the file determine what is added to the list.

If the template has settings that are visible and can be edited by the developer, then the *Settings* button becomes active when the template is selected. Clicking this button opens the Authentication Settings dialog box.

6. In the WebFOCUS Environments Properties dialog box, click *WebFOCUS* to test the connection.

The WebFOCUS Logon dialog box opens.

7. Type the user ID and password specified in step 5, and click *Logon*.

An unsuccessful sign-in is indicated by a prompt dialog box containing the logon template description in the Authentication field. This can occur if you typed your password incorrectly, if there is a problem with the security system, or if the logon template is improperly designed.

When you click *OK* to save the environment, the information associated with that template is written into the App Studio personalization file, which is stored on your local machine, such as:

`drive:\Users\user_id\AppData\Roaming\Information Builders\wfscom.xml`

where:

`user_id`

Is your Windows user ID.

## Creating a Custom Template

The template file is an xml file named dssso.xml in the *drive:\ibi\AppStudio82\bin* directory.

All of the custom logon templates are placed in this file:

- ❑ All templates are included within the opening <authentications> xml tag and the closing </authentications> xml tag.
- ❑ Each individual template is placed within its own opening <authentication> and closing </authentication> tags. Within these tags, each template is given a name and a description. The description displays in the Web Component Authentication section of the WebFOCUS Environment Properties dialog box.

The following describes all of the tags needed for a template file. All of the mandatory tags are required even if they have no attribute value specified, in which case the attribute assumes a default value. For clarity, you should specify all attributes, even those in which you do not change the default value.

### **Syntax:** How to Start a Logon Template File

These tags are mandatory.

```
<?xml version="1.0" encoding="utf-8"?>
<authentications>
```

### **Syntax:** How to Start an Individual Template Definition

This tag is mandatory.

```
<authentication name="form1" desc="Description of Form 1">
```

where:

*form1*

Is a name for the template.

*Description of Form 1*

Is the name that displays on the Web Component Authentication list. If this attribute is omitted, the value for the *name* attribute displays.

### **Syntax:** How to Specify Attributes for Accessing the Logon Resource

These tags are mandatory.



```

<sso_logon_resource desc="Logon Resource" read_only="true"
visible="true">
  <protocol default="%%environment%%" />
  <host default="%%environment%%" />
  <port default="%%environment%%" />
  <path desc="Description of path" default="resource_uri" />
</sso_logon_resource>

```

where:

*sso\_logon\_resource*

Is the URL of the program that will log users on to the SSO product. For example, this program may be a jsp, servlet, active server page, or CGI.

*Logon Resource*

Is the description that displays in the Web Component Authentication list, in the WebFOCUS Environments Properties dialog box.

*read\_only="true"*

Values are true and false. True specifies that the value can be changed in the WebFOCUS Environments Properties dialog box, while false specifies that it cannot be edited. The default value is true.

*visible="true"*

Values are true and false. True specifies that the value can be viewed in the WebFOCUS Environments Properties dialog box, while false specifies that it cannot be viewed. The default value is true.

*protocol*

Is the protocol to use to get to the logon resource, either http or https.

*hostname*

Is the host name of the logon resource.

*port\_number*

Is the port number of the logon resource. When the default attribute is not specified, no explicit port value will be used in the connection. The effective port, in this case, depends on the protocol value. If the protocol is http, then the port will be 80. If the protocol is https, then the port is 443. A forward slash (/) is prepended to the value of the default keyword if the value does not begin with one.

`%%environment%%`

Is a template variable that is replaced at run time by the corresponding value found in the Web Component Environment dialog box.

`resource_uri`

Is the part of the URL that follows the port and specifies the path to the logon resource.

### **Syntax:** How to Specify the Logon Result

These tags are mandatory.

The logon result will be a cookie if the sign-in was successful. If the sign-in was not successful, no cookie should be returned by the security system, which indicates to App Studio that the sign-in failed. In this case, a logon dialog box opens that allows the user to re-enter the user ID and password.

If a cookie is returned, the sign-in is assumed to be successful and the cookie is forwarded to WebFOCUS on every request. To describe the cookie required for authentication, add the following tags to the template:

```
<logon_result name="cookie_name" type="cookie" visible="false" />
```

where:

`cookie_name`

Is the name of the cookie returned by the logon resource. This name is case-sensitive.

`type=cookie`

Indicates what the App Studio software should expect as the result of a successful sign-in. If omitted, it defaults to `cookie`.

`visible="false"`

True specifies that the value can be viewed in the App Studio Environments window, false that it cannot. The default value is false.

### **Syntax:** How to Specify Required Logon Parameters

These tags are mandatory.

```
<user name="user" desc="user Id" default="%%environment%%"  
read_only="true" visible="true" />  
<password name="password" desc="Password" default="%%environment%%"  
read_only="true" visible="true" />
```

where:

*user*

Is the authenticated user ID. Note that this value is established as read-only and is taken from the Web Component Environment dialog box, by default.

*user Id*

Is the name that displays in the Web Component Authentication list, in the WebFOCUS Environments Properties dialog box. If this attribute is omitted, the value for the *user name* attribute displays.

`%%environment%%`

Is a template variable that is replaced at run time by the corresponding value found in the Web Component Environment dialog box.

`read_only="true"`

Values are true and false. True specifies that the value can be changed in the WebFOCUS Environments Properties dialog box, while false specifies that it cannot be edited. The default value is true.

`visible="true"`

Values are true and false. True specifies that the value can be viewed in the WebFOCUS Environments Properties dialog box, while false specifies that it cannot be viewed. The default value is true.

*password*

Is the authenticated password. Note that this value is established as read-only and, by default, is taken from the Web Component Environment dialog box. The value does not display, even if the visible property is specified.

*Password*

Is the name that displays in the Web Component Authentication list, in the WebFOCUS Environments Properties dialog box. If this attribute is omitted, the value for the *password name* attribute displays.

### **Syntax:**      **How to Specify Optional Logon Parameters**

The need for additional variables is determined by what you need to process a sign-on (in addition to a user ID and password).

```
<variable name="var1" default="initial_value" read_only="false"
visible="true"/>
<variable name="var2" read_only="false" visible="true">
  <protocol default="%%environment%%" />
  <host default="%%environment%%" />
  <port default="%%environment%%" />
  <path default="resource_uri" />
</variable>
```

where:

*var1*

Is a name for the additional variable required by the security system.

*initial\_value*

Is a default value for the variable.

*read\_only="false"*

Values are true and false. True specifies that the value can be changed in the WebFOCUS Environments Properties dialog box, while false specifies that it cannot be edited. The default value is false.

*visible="true"*

Values are true and false. True specifies that the value can be viewed in the WebFOCUS Environments Properties dialog box, while false specifies that it cannot be viewed. The default value is true for the variable name tag and false for the protocol, host, port, and path tags.

*protocol*

Is used to specify the protocol if the SSO product needs environment information for the additional variable. For more context, see the description of the sso\_logon\_resource tag.

*hostname*

Is used to specify the host name if the SSO product needs environment information for the additional variable. For more context, see the description of the sso\_logon\_resource tag.

*port\_number*

Is used to specify the port number if the SSO product needs environment information for the additional variable. For more context, see the description of the sso\_logon\_resource tag.

*%%environment%%*

Is a template variable that is replaced at run time by the corresponding value found in the Web Component Environment dialog box.

*resource\_uri*

Is used to specify the resource URL if the SSO product needs environment information for the additional variable. For more context, see the description of the sso\_logon\_resource tag.

### **Syntax:** How to Add User-Specified Cookies

By default, the App Studio software deletes cookie information when a user exits or when a user signs out. To preserve user-specified cookies, the cookie names must be specified using a cookie exception list in the template file. This list can be added to an existing template or a new template can be created to store just the cookie list. There is no limit on the number of cookies that can be specified.

```
<cookie_exclude_list>
  <variable name="var1" default="cookie_name" visible="true"/>
</cookie_exclude_list>
```

*var1*

Is a parameter name for the cookie.

*cookie\_name*

Is the name of the cookie. If this value is blank or contains a sample name for display purposes, the developer must specify the required cookie name in the Authentication Settings dialog box.

*visible="true"*

Values are true and false. True specifies that the value can be viewed in the WebFOCUS Environments Properties dialog box, while false specifies that it cannot be viewed. The default value is true.

### **Syntax:** How to End an Individual Template Definition

This tag is mandatory.

```
</authentication>
```

### **Syntax:** How to End the Template Definitions File

This tag is mandatory.

```
</authentications>
```

**Example: Sample Template File**

The TIBCO App Studio product comes with several sample templates in its template file. The following example shows the SiteMinder sample logon template. Note that:

- ❑ The name of the logon resource is *ibi\_sm*. The description that displays in the Web Component Authentication dialog box is *SiteMinder*.
- ❑ The URL information is taken from the Web Component dialog box and the URL is */siteminderagent/forms/login.fcc*.
- ❑ The logon result is a cookie named *SMSESSION*. Two variables, *SMAUTHREASON* and *TARGET*, are required. *TARGET* provides URL information for the WebFOCUS home page.

```
<authentication name="ibi_sm" desc="SiteMinder">
  <sso_logon_resource desc="Logon Resource" read_only="false"
visible="false">
    <protocol default="%%environment%%" />
    <host default="%%environment%%" />
    <port default="%%environment%%" />
    <path desc=" " default="/siteminderagent/forms/login.fcc" />
  </sso_logon_resource>
  <user name="user" desc="User Id" default="%%environment%%"
    read_only="true" visible="true" />
  <password name="password" desc="Password" default="%%environment%%"
    read_only="true" visible="true" />
  <logon_result name="SMSESSION" type="cookie" />
  <variable name="SMAUTHREASON" default="0" read_only="true"
    visible="true" />
  <variable name="TARGET" read_only="false" visible="true">
    <protocol default="%%environment%%" />
    <host default="%%environment%%" />
    <port default="%%environment%%" />
    <path default="/ibi_html/index.html" />
  </variable>
</authentication>
```

**Example: Sample Template With a Cookie Exclude List**

The following example illustrates a SiteMinder template with a cookie exception list.

```

<authentication name="ibi_sm" desc="SiteMinder">
  <sso_logon_resource desc="Logon Resource" read_only="false" visible="false">
    <protocol default="%%environment%%"/>
    <host default="%%environment%%"/>
    <port default="%%environment%%"/>
    <path desc="default="/siteminderagent/forms/login.fcc"/>
  </sso_logon_resource>
  <user name="user" desc="User Id" default="%%environment%%"
    read_only="true" visible="true"/>
  <password name="password" desc="Password" default="%%environment%%"
    read_only="true" visible="true"/>
  <logon_result name="SMSESSION" type="cookie"/>
  <variable name="SMAUTHREASON" default="0" read_only="true" visible="true"/>
  <variable name="TARGET" read_only="false" visible="true">
    <protocol default="%%environment%%"/>
    <host default="%%environment%%"/>
    <port default="%%environment%%"/>
    <path default="/ibi_html/index.html"/>
  </variable>
  <cookie_exclude_list>
    <variable name="ExcludeCookie1" visible="true">CookieName1</variable>
    <variable name="ExcludeCookie2" visible="true">CookieName2</variable>
    <variable name="ExcludeCookie3" visible="true">CookieName3</variable>
  </cookie_exclude_list>
</authentication>

```

When SiteMinder is selected as the Web Authentication component in the WebFOCUS Environment Properties dialog box, the Authentication Settings dialog box appears, as shown in the following image.

Parameter	Value
<b>Settings</b>	
user	admin
password	admin
SMAUTHREASON	0
TARGET	HTTP://8080/ibi_html/index.html
ExcludeCookie1	CookieName1
ExcludeCookie2	CookieName2
ExcludeCookie3	CookieName3

**Example:** Sample Template With a Cookie Exclude List and No Sign-In Request

The following example illustrates a template called Cookie\_save\_list and disables the sign-in request by setting the sso\_logon\_resource parameter to NONE.

```
<authentication name="ibi_Preserve_Cookies_Template"
  desc="Cookie_save_list">
  <sso_logon_resource desc="Logon Resource" read_only="false"
    visible="false">NONE </sso_logon_resource>
  <user name="user" desc="User's Name" default="%%environment%%"
    read_only="true" visible="true"/>
  <password name="password" desc="User's Password"
    default="%%environment%%" read_only="true" visible="true" />

<cookie_exclude_list>
  <variable name="ExcludeCookie1" default="CookieName1"
    visible="true"/>
  <variable name="ExcludeCookie2" default="CookieName2"
    visible="true"/>
  <variable name="ExcludeCookie3" default="CookieName3"
    visible="true"/>
  <variable name="ExcludeCookie4" default="CookieName4"
    visible="true"/>
</cookie_exclude_list>
</authentication>
```

## Configuring App Studio to Support IBM Tivoli Access Manager WebSEAL

App Studio software can connect to WebSEAL protected environments that use the HTML forms-based authentication scheme. App Studio includes a logon template for posting credentials to a WebSEAL login form and for adding a WebSEAL junction name. To configure App Studio to support WebSEAL, you must:

- ❑ Add a WebFOCUS Environment in App Studio that specifies the WebSEAL configuration information. For more information, see [How to Add a WebSEAL Environment in App Studio](#) on page 701. If a WebSEAL environment exists in App Studio from a previous configuration, we recommend that you delete these environments, restart App Studio, and recreate them. This ensures that the environment configuration file (wfscom.xml) is updated with the correct WebFOCUS Environment information.
- ❑ Manually add the WebSEAL junction name in the App Studio template file (dssso.xml), which stores the configuration information for different types of vendors. The junction name is stored in the WebFOCUS Environments configuration file after adding an environment to App Studio. For more information on adding the WebSEAL junction name to the dssso.xml file, see [How to Add the WebSEAL Junction Name in the App Studio Template Logon File](#) on page 704.
- ❑ If necessary, change the communication protocol in the Logon Template. By default, the WebSEAL Logon Template is configured to use HTTPS communication. If your WebSEAL environment uses HTTP, see [How to Modify the Standard WebSEAL Logon Template for HTTP Connections](#) on page 703.



Before configuring App Studio, you need to configure WebSEAL to protect WebFOCUS and verify that you can access WebFOCUS successfully from your web browser.

### **Procedure:** How to Add a WebSEAL Environment in App Studio

By default, the standard WebSEAL Logon Template uses PD-S-SESSION-ID as the name of the cookie returned by the logon resource. This cookie is used for WebSEAL connections that use the HTTPS protocol.

**Note:** If your WebSEAL environment is using the HTTP protocol, see [How to Modify the Standard WebSEAL Logon Template for HTTP Connections](#) on page 703.

1. From the App Studio Environment Properties dialog box, click the *Web Component* object and specify a value for each of the following:
  - ☐ **Host Name/IP Address.** Specify the server name or IP address on which the WebSEAL web server is installed.
  - ☐ **Protocol.** Specify *HTTP* or *HTTPS* as the value.
  - ☐ **HTML Alias.** Enter the alias defined on the web server for the `ibi_html` directory. If your WebFOCUS environment does not use the default alias (`/ibi_apps/ibi_html`), uncheck the *HTML Alias* check box and specify the custom alias defined on the remote web server.
  - ☐ **Port.** Specify the WebSEAL web server port number.
  - ☐ **Client Path.** Specifies how calls are made from App Studio to the web server. By default, when you add a new WebFOCUS environment, it is set to use the WebFOCUS Servlet with the default `ibi_apps` context path:

`/ibi_apps/WFServlet`

where:

`ibi_apps`

Is customizable.

`WFServlet`

Is constant.

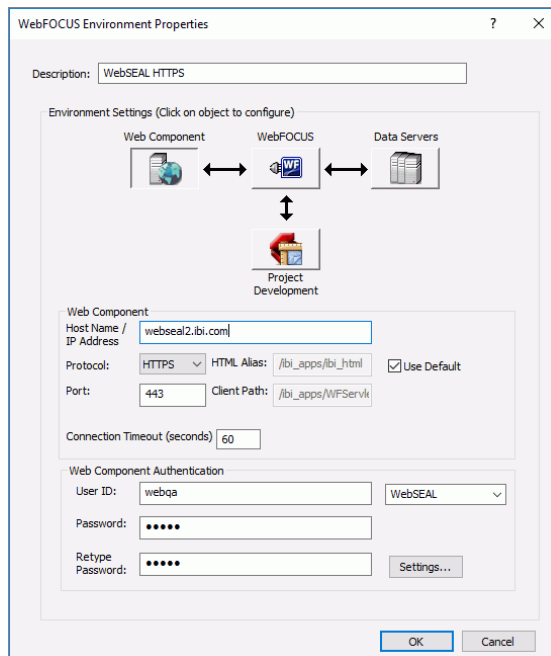
If the WebFOCUS environment uses a non-default context path, deselect the *Use Default* check box and provide the correct Client Path. For example:

`/ibi_apps8/WFServlet`

If the Client Path is incorrect for the environment, you receive an error when you click the WebFOCUS button at the top of the page or when you press OK to exit and save your changes. If you do not know your path, ask your WebFOCUS Administrator or check the Administration Console of the WebFOCUS environment to which you want to connect. The Client Path settings for the environment are located under *Utilities* and *Client Selection*.

- ☐ **Connection Timeout (seconds).** Enter the number of seconds that App Studio should wait for a response from the server before it cancels the connection.
- ☐ **User ID.** Enter a valid user ID to connect to the WebSEAL web server. Select *WebSEAL* from the drop-down box next to the *User ID* input box.
- ☐ **Password.** Enter a valid password to connect to the WebSEAL web server.
- ☐ **Retype Password.** Enter the password again for verification purposes.

The Web Component configuration options, with sample values, are shown in the following image.



2. Click the *Settings* button.

3. Verify, and edit if necessary, to make sure the Logon Resource field matches the host, protocol, port, and path to your WebSEAL logon form. The following image shows the Authentication Settings dialog box with sample values.

Parameter	Value
Settings	
username	webqa
password	----
login-form-type	pwd
junction_path	

OK Cancel

The App Studio environment properties dialog box shows the form variables that will be posted to the logon form before attempting to connect with WebFOCUS. Note that the credentials displayed in this dialog box cannot be edited.

**Note:** You can control how App Studio generates the default Logon Resource values shown in this dialog box. For example, you can change the protocol to always be "https" or set the path to a custom value.

4. Type the WebSEAL junction name in the *junction path* input box and click OK.
- Note:** If a value was specified in the dssso.xml file, it is displayed in the junction path input box. Also, the value must be preceded by a forward slash (/).
5. To configure the other Objects in the Environment Settings dialog box, refer to the *TIBCO WebFOCUS® App Studio Installation and Configuration Guide*.
6. Click OK and then click OK again to save the properties.

You may be prompted once more for your WebSEAL credentials to complete the save operation.

After the dialog box closes, your environment is added to the WebFOCUS Environment tree where you can work with it.

### **Procedure:** How to Modify the Standard WebSEAL Logon Template for HTTP Connections

If you are using the HTTP protocol with your WebSEAL environment, you need to perform the following steps to modify the standard WebSEAL Logon Template.

1. Make a backup copy of the following file:

*drive:\ibi\AppStudio<sup>nn</sup>\bin\dssso.xml*

where:

*drive*

Is the directory in which App Studio is installed.

*nn*

Is the App Studio release number.

2. Open the original dssso.xml file in a text editor and search for "ibi\_webseal".
3. Copy the entire <authentication> block surrounding "ibi\_webseal" and paste it just above the </authentications> line at the bottom of the file.
4. Inside the new <authentication> block, change the name and description to unique values, for example, "webseal\_http" for the name and "WebSEALHTTP" for the description.
5. In the <authentication> block, locate the following line and change "PD-S-SESSION-ID" to "PD-H-SESSION-ID".

```
<logon_result name="PD-S-SESSION-ID" type="cookie" />
```

This enables the HTTP protocol to be used for the WebSEAL connection.

6. Save the changes to the file.
7. When configuring App Studio to communicate with the WebSEAL protected WebFOCUS environment, select *WebSEALHTTP* from the Web Component Authentication drop-down list.

### **Procedure:** How to Add the WebSEAL Junction Name in the App Studio Template Logon File

1. Edit the *drive:\ibi\AppStudio<sup>nn</sup>\bin\dssso.xml* file.

where:

*drive*

Is the directory in which App Studio is installed.

*nn*

Is the App Studio release number.

2. Locate the WebSEAL configuration information in the file:

```

<authentication name="ibi_webseal" desc="WebSEAL">
  <sso_logon_resource desc="Logon Resource" read_only="false"
visible="false">
    <protocol default="%%environment%%" />
    <host default="%%environment%%"/>
    <port default="%%environment%%" />
    <path desc="" default="/pkmslogin.form" />
    <logout_command default="/pkmslogout" />
    <logout_before_login default="no" />
  </sso_logon_resource>
  <user name="username" desc="Username" default="%%environment%%"
read_only="true" visible="true" />
  <password name="password" desc="Password" default="%%environment%%"
read_only="true" visible="true" />
  <logon_result name="PD-S-SESSION-ID" type="cookie" />
  <variable name="login-form-type" default="pwd" read_only="true"
visible="true" /><variable name="junction_path" default = ""
desc="junction path" visible="true"/>

```

3. Update the following syntax,

```

<variable name="junction_path" default = "" desc="junction path"
visible="true"/>

```

as follows:

```

<variable name="junction_path" default = "/my_junction_name"
desc="junction path" visible="true"/>

```

where:

`/my_junction_name`

Is the junction configured in the WebSEAL server.

4. Save your changes and close the dssso.xml file.

## Additional WebSEAL Configuration Steps

In order for WebFOCUS, ReportCaster, and App Studio to function successfully with WebSEAL, some additional WebSEAL settings are necessary.

In the WebSEAL instance configuration file, change the following settings from the default:

- ☐ Set `dynurl-allow-large-posts` = yes (Some of the WebFOCUS generated URL strings are long. This setting prevents the URLs from being truncated.)
- ☐ Set `resend-webseal-cookies` = yes (Without this setting, WebFOCUS and ReportCaster may lose the value of the WebSEAL cookie.)

- ❑ Set `jmt-map = lib/jmt.conf` (This mapping is necessary due to the way WebFOCUS rewrites URLs and loses the junction name.)

### Creating the `jmt.conf` File

The `jmt.conf` file must be created because it does not exist, by default. The file should be created under the `server-root/lib` directory. The "server-root" is defined in the WebSEAL instance configuration file. The `jmt.conf` file should contain the following lines:

```
/junctionname /ibi_apps/*
```

```
/junctionname /rcaster/*
```

```
/junctionname /ibi_html/*
```

```
/junctionname /approot/*
```

**Note:** `/junctionname` should be replaced with the name of the junction that is being used. If WebFOCUS was not configured with the default context roots, be sure to specify the context roots accordingly in this file.

## Manipulating TIBCO WebFOCUS Variables

---

WebFOCUS variables control WebFOCUS processing. The Administration Console gives you the ability to view and change a wide variety of WebFOCUS variables. To further manipulate these variables, WebFOCUS provides:

- ❑ A scripting language that enables you to set variable values based on conditions and control processing options for those variables.
- ❑ A plug-in for the Servlet version of the WebFOCUS Client that provides methods for copying variables between the WebFOCUS variable table and the HTTP header or application session.

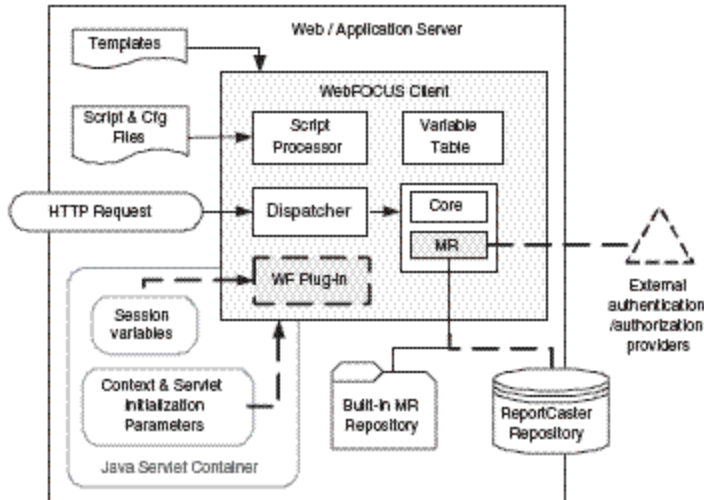
### **In this appendix:**

- ❑ [Customizing TIBCO WebFOCUS Request Processing](#)
  - ❑ [TIBCO WebFOCUS Script and Configuration Files](#)
  - ❑ [TIBCO WebFOCUS Variables](#)
  - ❑ [TIBCO WebFOCUS Script Commands](#)
  - ❑ [TIBCO WebFOCUS Servlet Plug-in](#)
  - ❑ [Managed Reporting Internal Variables](#)
  - ❑ [HTTP Header Variables Available for Script Processing](#)
- 

### **Customizing TIBCO WebFOCUS Request Processing**

The WebFOCUS application can be configured and extended to work with a wide variety of third-party products or customized solutions.

The following diagram illustrates the points in the WebFOCUS Client processing at which customization can be implemented.



The WebFOCUS Client has two points at which customized programs can be used to extend its default processing:

- ❑ A Java Servlet filter can be called before each HTTP request is passed to the WebFOCUS application. The HTTP Client (for example, a web browser) sends the request to the web server, which then passes the request to the application server. The Java Servlet filter can intercept the call from the application server to the WebFOCUS application, and can alter the request, respond, or halt execution before the WebFOCUS application receives it. For example, the Java Servlet filter may be used to perform custom authentication.
- ❑ The WebFOCUS plug-in can be called before each request is passed to the WebFOCUS Reporting Server, whether it is a self-service or Managed Reporting request. Plug-in code can also be called prior to passing results from the WebFOCUS Reporting Server to the WebFOCUS Client. This gives you the opportunity to preprocess a request from the browser and post-process the response before returning the result to the browser.

To use the WebFOCUS plug-in, the customer site must perform some configuration steps, such as setting WebFOCUS variable values or editing properties. The plug-in provides methods for copying WebFOCUS variables, application server session variables, and HTTP header variables between the WebFOCUS variable table, the application server session, and the HTTP header. For instructions on using this plug-in, see [TIBCO WebFOCUS Servlet Plug-in](#) on page 715.



If you require preprocessing or post-processing methods not included in the supplied plug-in, you can develop your own plug-in. You should extend the class for the existing plug-in, so that you can still use its methods. A plug-in for the Servlet version of the WebFOCUS Client must be written in the Java language.

On the WebFOCUS Reporting Server, custom programs similar to WebFOCUS Client plug-ins are referred to as exits. The WebFOCUS Reporting Server has two exits that can be used by WebFOCUS:

- ❑ **Pre-Verify User ID Exit (PVUIDXT).** This exit is used to customize WebFOCUS Reporting Server authentication. It can be used to perform the following tasks:
  - ❑ Configure the WebFOCUS Reporting Server to authenticate against a third-party directory.
  - ❑ Enable a WebFOCUS Reporting Server or hub server to establish a secure connection from another WebFOCUS Reporting Server or the WebFOCUS Client, without checking credentials. In this case, credentials have already been verified at an earlier point.
  - ❑ Enable a WebFOCUS Reporting Server or hub server to establish a secure connection to another WebFOCUS Reporting Server by replacing a verified user ID with a user ID appropriate for the latter server.
- ❑ **WebFOCUS DBA Exit.** This exit enables WebFOCUS metadata to use replaceable parameters for data source security. It is typically used to limit the values in a data source to which a user has access.

## TIBCO WebFOCUS Script and Configuration Files

WebFOCUS uses configuration files and script files in processing a request. The WebFOCUS Client uses the variable values set in these files for local processing and for processing requests.

For each type of request, the files are processed in a specific order. Each file can modify the variable values in the WebFOCUS variable table.

For a detailed description of the WebFOCUS Client configuration files, see [TIBCO WebFOCUS Client Configuration Files](#) on page 511.

## TIBCO WebFOCUS Variables

The internal variables that control the processing behavior of the WebFOCUS Client are loaded into a memory-resident table from several sources, including:

- ❑ **WebFOCUS script and configuration files.** The WebFOCUS Client has a set of script and configuration files (\*.wfs, \*.prf, \*.cfg) containing information that defines its operation. For example, variables identify user IDs, host names, host ports, and directory locations.

Configuration files (\*.cfg) provide initialization parameters that define the environment of each request. Initialization parameters consist of *name=value* pairs.

Script files (\*.wfs, \*.prf) define WebFOCUS variables that are used during processing. You can use the WebFOCUS scripting language to modify the variable values based on conditional logic.

- ❑ **Template files and HTML pages.** Template files describe page layouts for pages that display the status of core processing and some Managed Reporting processing, such as the deferred status page.
- ❑ **HTTP headers.** HTTP variables are passed between a web server and browser in the HTTP request/response header. HTTP variables typically define the environment of the web browser. For example, the HTTP\_USER\_AGENT header defines the browser manufacturer and version. The WebFOCUS Client can use any of the standard HTTP variables that are created and populated by the web server and the web browser.

## TIBCO WebFOCUS Variable Table

The memory resident WebFOCUS variable table holds variables, allowing them to be used for local processing and in the communication between WebFOCUS components.

You can use the Administration Console to change the values of most WebFOCUS variables. For more information about the Administration Console, see [Configuring the TIBCO WebFOCUS Client](#) on page 61.

## TIBCO WebFOCUS Script Commands

You can use WebFOCUS script (WFS) commands with WebFOCUS Client settings and HTTP header variables (see [HTTP Header Variables Available for Script Processing](#) on page 725) to further customize processing and control of the WebFOCUS Client.

You can use WFS commands to:

- ❑ Define, validate, and control WebFOCUS Client variables.

- ☐ Invoke WebFOCUS plug-ins.
- ☐ Send information, such as FOCEXEC names and descriptions, to the WebFOCUS Reporting Server.

**Tip:** You can also use the following variables with WebFOCUS script commands:

- ☐ **Form variables.** Set from an HTML page. Form variables are automatically sent to the WebFOCUS Reporting Server, unless they begin with *IBI* or *WF*.
- ☐ **Output variables.** Set by the WebFOCUS Reporting Server and passed back to the WebFOCUS Client.

### **Reference:** WFS Command Syntax

You can place the following WFS commands in the site.wfs file, found at *drive:\ibi\WebFOCUS82\client\wfc\etc*.

Command Syntax	Description
<code>&lt;EXIT&gt;</code>	Causes the WebFOCUS Client to stop processing and exit immediately.
<code>&lt;INCLUDE&gt; <i>filename</i></code>	Incorporates WFS logic from external files into standard WFS processing. The file must exist for processing to continue. For more information, see <a href="#">How to Include External Files in Standard WFS Processing</a> on page 715.
<code>&lt;CONDITIONAL_INCLUDE&gt; <i>filename</i></code>	Works in the same manner as <code>&lt;INCLUDE&gt; <i>filename</i></code> , except that the file does not need to exist. For more information, see <a href="#">How to Include External Files in Standard WFS Processing</a> on page 715.
<code>&lt;SET&gt; <i>variable</i> (<i>option</i>)</code>	Sends variables to the WebFOCUS Reporting Server for use with server procedures. It is used for variables that are not automatically sent to the Reporting Server. For more information, see <a href="#">How to Send Variables to the TIBCO WebFOCUS Reporting Server</a> on page 723.

Command Syntax	Description
<code>&lt;CALL&gt; function(<i>parml</i>,...)</code>	Invokes WebFOCUS plug-ins. Each WebFOCUS plug-in can contain a maximum of ten input parameters. For more information, see <a href="#">How to Invoke the TIBCO WebFOCUS Servlet Plug-in</a> on page 716.
<code>&lt;IF&gt; variable operator value &lt;ELSE&gt; &lt;ENDIF&gt;</code>	Allows the conditional checking of WebFOCUS Client variables. For more information, see <a href="#">How to Conditionally Check Variables</a> on page 721.
<code>&lt;IFDEF&gt; variable &lt;ELSE&gt; &lt;ENDIF&gt;</code>	Checks for the existence of a WebFOCUS Client variable. For more information, see <a href="#">How to Check for the Existence of a Variable</a> on page 722.
<code>&lt;IFNDEF&gt; variable &lt;ELSE&gt; &lt;ENDIF&gt;</code>	Checks to see whether a WebFOCUS Client variable does not exist. For more information, see <a href="#">How to Check Whether a Variable Does Not Exist</a> on page 722.
<code>&lt;SENDVAR&gt; name={constant  &amp;value} &lt;ENDSENDVAR&gt;</code>	<p>Sends variables to the WebFOCUS Reporting Server for use with server procedures. It is used for variables that are not automatically sent to the Reporting Server. For more information, see <a href="#">How to Send Variables to the TIBCO WebFOCUS Reporting Server</a> on page 723.</p> <p><b>Note:</b> This syntax has been deprecated. It is recommended that the <code>&lt;SET&gt; variable_name (pass)</code> is used, instead of the <code>&lt;SENDVAR&gt;</code> technique.</p>

**Reference: WFS Language Syntax**

When coding WFS commands, you can use the following syntax.

Command Syntax	Description
<pre>&lt;! &gt; #</pre>	<p>Comment characters that tell the WebFOCUS Client that the current line is a comment. The less than sign and exclamation point (&lt;!) or hash (#) sign must be the first characters in the line. For example:</p> <pre>&lt;! This is a comment.&gt; # This is also a comment.</pre>
<pre>\\=</pre>	<p>Continuation character that you can add at the end of any line. It tells the WebFOCUS Client that the next line is a continuation of the current line.</p>
<pre>\n</pre>	<p>Carriage return line feed that enables you to put multiple commands on a single line.</p>

Command Syntax	Description
<code>value = {<i>constant</i> &amp;<i>variable</i>}</code>	<p>Assigns a value to a variable in a WFS file as either a constant or a variable, where:</p> <p><i>constant</i></p> <p>Is a literal value. If you include quotation marks ("), they are passed as part of the variable.</p> <p><b>Note:</b> If the constant contains special characters, for example, an ampersand (&amp;) or backslash (\), the backslash character (\) can be used as an escape character, to ensure that the special character is passed as part of the value.</p> <p><i>&amp;variable</i></p> <p>Is a placeholder for a value.</p> <p>Once a variable has been assigned a value, you can use the variable name, prefixed with an ampersand (&amp;), in place of the value. You can concatenate literal values in this way. For example:</p> <pre>long_string = this is a long_string = &amp;long_string very long string long_string = &amp;long_string that requires multiple lines</pre>

**Reference:** Backslash Escape Character

When a backslash (\) is used as the escape character, you can:

- ❑ Include a string delimiter, such as a single quotation mark ('), as part of the value within the string. If you precede the character with a backslash (\), the character is interpreted as data, not as the end-of-string delimiter.
- ❑ Include a backslash (\) as part of the value within the string. You can precede the backslash (\) with a second backslash (\).

When a backslash (\) is used as an escape character, it is not included in calculations based on the length of the string. A string of five characters and one escape character fits into a five-character variable.

**Syntax:**      **How to Include External Files in Standard WFS Processing**

You can incorporate external files into standard WFS processing. The following `<INCLUDE>` command allows another WFS file to be called from standard WFS files. The custom file must exist for processing to continue. The `<CONDITIONAL_INCLUDE>` *filename* command works in the same manner as the `<INCLUDE>` *filename* command, except that the file does not need to exist.

```
<INCLUDE> filename
```

```
<CONDITIONAL_INCLUDE> filename
```

where:

*filename*

Is the name of the file to be included for WFS processing.

**Example:**      **Including External Files in Standard WFS Processing**

The following command includes a file called custom.wfs in the client/wfc/etc directory, specified by the `&CGI_BASE_DIR` variable. This file must exist for processing to continue.

```
_exit=custom.wfs
```

```
-<INCLUDE> &CGI_BASE_DIR&_exit
```

The following conditional include command checks for a file called custom.wfs in the client/wfc/etc directory, specified by the `&CGI_BASE_DIR` variable.

```
_exit=custom.wfs
```

```
-<CONDITIONAL_INCLUDE> &CGI_BASE_DIR&_exit
```

**TIBCO WebFOCUS Servlet Plug-in**

The TIBCO WebFOCUS Servlet plug-in contains methods for manipulating WebFOCUS variables. Since the parameters passed to each of these methods cannot be literal values, the values must first be placed into variables, where they can then be used in the method call.

For a list of HTTP header variables placed in the WebFOCUS variable table, see [HTTP Header Variables Available for Script Processing](#) on page 725.

**Procedure: How to Enable the TIBCO WebFOCUS Servlet Plug-in**

The TIBCO WebFOCUS Servlet plug-in is enabled by setting the WFEXT variable to the class name `ibi.webfoc.WFEXTDefault` in the `webfocus.cfg` file.

1. In the Security Center, on the Configuration tab, under the Application Settings folder, click *Client Settings*.
2. If the class name `ibi.webfoc.WFEXTDefault` is not displayed as the value of the Plugin Class (IBI\_WFEXT) setting, type it, and then click Save.

**Note:** Only one plug-in can be active at a time. If you need to add additional functionality, you should extend this class to include your functionality, so that you do not lose access to the methods provided in this class.

**Syntax: How to Invoke the TIBCO WebFOCUS Servlet Plug-in**

The following `<CALL>` command invokes a WebFOCUS plug-in.

```
<CALL> routine(parm1,parm2)  
<IF> RETCODE NE "returncodevalue"  
# insert your code here  
<ENDIF>
```

where:

`<CALL>`

Is the command that invokes the WebFOCUS Servlet plug-in.

*routine*

Defines the name of the actual function to be called (for example, `security` or `CopyHTTPCookieToWFVar`).

*(parm1,parm2)*

Are the input parameters of the WebFOCUS plug-in. Each WebFOCUS plug-in can contain a maximum of ten input parameters. The output buffer is passed, but does not contribute to the maximum number of input parameters.

RETCODE

Is the status of the method call.

*returncodevalue*

Is the value you are comparing to what the plug-in returns (for example, 0).



## CopyHTTPHeaderToWFVar Method

The CopyHTTPHeaderToWFVar method copies the value of an HTTP Header variable into a WebFOCUS Servlet variable.

### **Example:** Using the CopyHTTPHeaderToWFVar Method

1. In the Administration Console, on the Configuration tab, click *Custom Settings* and in the Custom Settings window type the following code:

```
HTTP_HEADER_NAME = hostWFS_VAR_NAME = WFV
<CALL> CopyHTTPHeaderToWFVar (HTTP_HEADER_NAME,WFS_VAR_NAME)
<SET> WFV (pass)
```

where:

`HTTP_HEADER_NAME`

Is the name of the HTTP header entry from which the value is retrieved.

`host`

Is the value retrieved.

`WFS_VAR_NAME`

Is the name of the WebFOCUS Servlet variable that receives the value.

`WFV`

Is the value assigned to the WebFOCUS Servlet variable.

A return code of 0 (zero) indicates success and 999 indicates failure.

2. Run the following procedure from within a Business Intelligence Portal (BIP):

```
-TYPE &WFV
```

The web server name in the HTTP header is copied into a WebFOCUS Servlet variable.

## CopyWFVarToSessionVar Method

The CopyWFVarToSessionVar method copies the value of a WebFOCUS Servlet variable into a web application session variable.

**Example: Using the CopyWFVarToSessionVar Method**

1. Navigate to the folder `drive:/ibi/WebFOCUS82/webapps/webfocus`, open a text editor, and type or copy and paste the following code:

```
<HTML>
<BODY>
Session variable value is <%= session.getAttribute("sampleVariable")%>
</BODY>
</HTML>
```

**Note:** The sample.jsp file uses the `session.getAttribute` method to retrieve the value of the web application session variable.

2. Save the file as `sample.jsp`, and close the text editor.
3. Sign in as an administrator.
4. In the Administration Console, on the Configuration tab, click *Custom Settings*, and then type the following code:

```
<IFDEF> IBIMR_user
SESSION_VAR_NAME = sampleVariable
WFS_VAR_NAME = &IBIMR_user
<CALL> CopyWFVarToSessionVar (WFS_VAR_NAME, SESSION_VAR_NAME)
<ENDIF>
```

where:

`WFS_VAR_NAME`

Is the name of the WebFOCUS Servlet variable. The value of this variable is the name of the actual WebFOCUS variable whose value is copied into the web application session variable.

`SESSION_VAR_NAME`

Is the name of the web application session variable.

This function always returns 0 (zero).

5. Click Save.
6. When you receive a message that the file was saved successfully, click *OK*.
7. Sign in to the BI Portal.
8. In the same browser window, type `http://hostname:port/ibi_apps/sample.jsp` in the address bar and press the Enter key.

When you run the `sample.jsp` file, the session variable displays the user ID you provided on the Sign in page.

## CopySessionVarToWFVar Method

The CopySessionVarToWFVar method copies the value of a web application session variable into a WebFOCUS Servlet variable.

### **Example:** Using the CopySessionVarToWFVar Method

1. Navigate to the folder `drive:/ibi/WebFOCUS82/webapps/webfocus`, open a text editor, and type or copy and paste the following code:

```
<%@ page language="java" contentType="text/html"%>
<% session.setAttribute("sampleVariable","sampleValue"); %>
```

**Note:** The sample.jsp file uses the session.setAttribute method to initialize a web application session variable.

2. Save the file as sample.jsp, and close the text editor.
3. Sign in as an administrator.
4. In the Administration Console, on the Configuration tab, click *Custom Settings*, and then type the following code:

```
SESSION_VAR_NAME = sampleVariable
WFS_VAR_NAME = WfV
<CALL> CopySessionVarToWFVar (SESSION_VAR_NAME,WFS_VAR_NAME)
<SET> WfV (pass)
```

where:

`SESSION_VAR_NAME`

Is the name of the web application session variable.

`WFS_VAR_NAME`

Is the name of the WebFOCUS Servlet variable that receives the value.

A return code of 0 (zero) indicates success and 999 indicates failure.

5. Run the following procedure from within a Business Intelligence Portal (BIP):

```
-TYPE &WfV
```

The application server session variable and its associated value are copied to the WebFOCUS Servlet variable and displayed.

## CopyHTTPMethodToWFVar Method

The CopyHTTPMethodToWFVar method copies a value representing the HTTP request type into a WebFOCUS Servlet variable. The request type is usually GET or POST.

### **Example:** Using the CopyHTTPMethodToWFVar Method

1. Sign in as an administrator.
2. In the Administration Console, on the Configuration tab, click *Custom Settings*, and then type the following code:

```
WFS_VAR_NAME = WFV
<CALL> CopyHTTPMethodToWFVar (WFS_VAR_NAME)
<SET> WFV (pass)
```

where:

`WFS_VAR_NAME`

Is the name of the WebFOCUS Servlet variable that receives the value.

A return code of 0 (zero) indicates success and 999 indicates failure.

3. Run the following procedure from within a Business Intelligence Portal (BIP):

```
-TYPE &WFV
```

Depending on how the WebFOCUS Servlet is called, a GET or POST operator is displayed.

## CopyHTTPCookieToWFVar Method

The CopyHTTPCookieToWFVar method copies the contents of an HTTP cookie into a WebFOCUS Servlet variable.

### **Example:** Using the CopyHTTPCookieToWFVar Method

1. Sign in as an administrator.
2. In the Administration Console, on the Configuration tab, click *Custom Settings*, and then type the following code:

```
COOKIE_NAME = WF_SESSIONID
WFS_VAR_NAME = WFV
<CALL> CopyHTTPCookieToWFVar (COOKIE_NAME,WFS_VAR_NAME)
<SET> WFV (pass)
```

where:

`COOKIE_NAME`

Is the name of the HTTP cookie from which the value is retrieved.

*WFS\_VAR\_NAME*

Is the name of the WebFOCUS Servlet variable that receives the value.

A return code of 0 (zero) indicates success and 999 indicates failure.

3. Run the following procedure from within a Business Intelligence Portal (BIP):

```
-TYPE &WFFV
```

The contents of an HTTP cookie are displayed. In this case, the HTTP cookie is the WF\_SESSIONID cookie.

### **Syntax:** How to Conditionally Check Variables

The following <IF> statement conditionally checks WebFOCUS Client variables.

```
<IF> variable operator value
<ELSE>
<ENDIF>
```

where:

*variable*

Is any WebFOCUS Client variable.

*operator*

Can be set to EQ, NE, CONTAINS, OR, or AND.

*value*

Applies to any WebFOCUS Client variable or constant.

### **Example:** Conditionally Checking Variables in Uppercase

You can use the following <IF> statement to ensure that the Sign in page is invoked.

If you add upper to a WFS variable, the value is checked as if it has all uppercase characters. This allows you to check the value that the user entered without worrying about the case.

The following <IF> statement ensures that any value entered is treated as uppercase.

```
<IF> ABC.upper EQ "Y" OR ABC.upper EQ "YES"
DEF = &GHI
<ENDIF>
```

The following <IF> statement ensures that any server value entered is not case-sensitive.

```
<IF> IBIC_server.upper EQ "EDASERV"
# INSERT YOUR CODE HERE....
<ENDIF>
```

The following <IF> statement checks whether or not the constant .ibi.com is contained in the WebFOCUS Client variable HTTP\_HOST.

```
<IF> HTTP_HOST contains ".ibi.com"  
# INSERT YOUR CODE HERE....  
<ENDIF>
```

### **Syntax:**      **How to Check for the Existence of a Variable**

The following <IFDEF> statement checks for the existence of a WebFOCUS Client variable.

```
<IFDEF> variable  
<ELSE>  
<ENDIF>
```

where:

*variable*

Is any WebFOCUS Client variable.

### **Example:**      **Checking for and Defining a Variable**

In the following example, if the variable \_ON\_NT exists, PATH\_SEP is set to a semicolon (;). If the variable \_ON\_NT does not exist, PATH\_SEP is set to a colon (:).

```
<IFDEF> _ON_NT  
PATH_SEP=;  
<ELSE> PATH_SEP=:  
<ENDIF>
```

### **Syntax:**      **How to Check Whether a Variable Does Not Exist**

The following <IFNDEF> statement checks to see whether a WebFOCUS Client variable does not exist.

```
<IFNDEF> variable  
<ELSE>  
<ENDIF>
```

where:

*variable*

Is any WebFOCUS Client variable.

**Syntax:**      **How to Send Variables to the TIBCO WebFOCUS Reporting Server**

The <SET> command sends variables to the WebFOCUS Reporting Server for use with server procedures. Certain custom variables are sent to the WebFOCUS Reporting Server automatically. This syntax is used for variables that are not automatically sent to the WebFOCUS Reporting Server.

```
<SET> name = {constant|&variable} (pass)
```

where:

*name*

Is a Dialogue Manager variable to be used by the WebFOCUS Reporting Server.

*constant*

Is a literal value. If you include quotation marks ("), they are passed in as part of the variable. Applies to any WebFOCUS Client variable.

*&variable*

Is a placeholder for a value. Applies to any WebFOCUS Client variable.

**Managed Reporting Internal Variables**

There are several variables related to Managed Reporting processing that you can pass to the Reporting Server. This may be useful for controlling processing flow or for display purposes in the report output. You can do this by configuring the <SET> *variable* (pass) commands in the Administration Console. Useful variables include:

- ☐ **IBIMR\_folder.** The folder where the processed report is stored.
- ☐ **IBIMR\_fullpath.** The complete path for a procedure, including file name and extension.
- ☐ **IBIMR\_user.** The user ID processing the report request.
- ☐ **IBIMR\_domain.** The domain HREF where the report being processed is stored.
- ☐ **MR\_FULL\_FEXNAME.** The description given to the report by the developer. This description is visible to users. When the report is run from the text editor or InfoAssist, the variable is not populated.
- ☐ **MR\_ITEM\_HANDLE.** The file name (also known as the IBFS name) assigned to the report when it was created. When the report is run from the text editor or the Report canvas in App Studio, the variable is set to *ADHOCRQ*.

### **Example:** Using Managed Reporting Internal Variables

1. Sign in as an administrator.
2. In the Administration Console, on the Configuration tab, click *Custom Settings*, then type the following code to the end of the file:

```
<SET> IBIMR_folder (pass)
<SET> IBIMR_fullpath (pass)
<SET> IBIMR_user (pass)
<SET> IBIMR_domain (pass)
<SET> MR_FULL_FEXNAME (pass)
<SET> MR_ITEM_HANDLE (pass)
```

**Note:** Do not write over the existing lines in Custom Settings. The file must begin with the <VER> line.

3. Click Save.
4. Sign in to Managed Reporting and use the text editor to create a standard report called *test2* in the default workspace.
5. Enter the following code and save the report:

```
-TYPE IBIMR_folder is &IBIMR_folder
-TYPE IBIMR_fullpath is &IBIMR_fullpath
-TYPE IBIMR_user is &IBIMR_user
-TYPE IBIMR_domain is &IBIMR_domain
-TYPE MR_FULL_FEXNAME is &MR_FULL_FEXNAME
-TYPE MR_ITEM_HANDLE is &MR_ITEM_HANDLE
```

6. Right-click the saved report and select *Properties* from the shortcut menu, then deselect the *Prompt for Parameters* option.
7. Change the description to *Test 2 Description*.
8. Save your changes and run the report.

The following output appears:

```
IBIMR_folder is Sales
IBIMR_fullpath is IBFS:/WFC/Repository/Retail/Sales/variables.fex
IBIMR_user is admin
IBIMR_domain is Retail/
MR_FULL_FEXNAME is variablesTitle
MR_ITEM_HANDLE is variables
```

When the report is run from the text editor, the following output appears:



```

IBIMR_folder is Sales
IBIMR_fullpath is IBFS:/WFC/Repository/Retail/Sales/*
IBIMR_user is admin
IBIMR_domain is Retail/
MR_FULL_FEXNAME is
MR_ITEM_HANDLE is ADHOCRQ

```

## HTTP Header Variables Available for Script Processing

You can use standard HTTP header variables to customize the processing and control of the WebFOCUS Client. Once the WebFOCUS Servlet places the variables in the WebFOCUS variable table, you can use the variables in the site.wfs file.

HTTP Header Variables	Description
<code>AUTH_TYPE</code>	Specifies the authentication scheme, if an authorization header is supplied.
<code>CONTENT_LENGTH</code>	Stores the number of bytes of data sent. For POST requests only.
<code>CONTENT_TYPE</code>	Designates the MIME type of attached data.
<code>DOCUMENT_ROOT</code>	Specifies the location of the host directory.
<code>HTTP_ACCEPT</code>	Specifies the media (MIME) type the WebFOCUS Client prefers to accept, separated by commas (,).
<code>HTTP_ACCEPT_ENCODING</code>	Restricts the content-codings that are acceptable in the response.
<code>HTTP_ACCEPT_LANGUAGE</code>	Indicates which languages are preferred.
<code>HTTP_USER_AGENT</code>	Identifies the browser (or other client) making the request. It can be used to return content to different browsers.
<code>HTTP_REFERER</code>	Indicates the URL of the referring webpage.
<code>PATH_INFO</code>	Supplies any path information attached to the URL after the server address, but before the query string.
<code>PATH_TRANSLATED</code>	Value of <code>PATH_INFO</code> with any virtual path name expanded into a directory specification.

HTTP Header Variables	Description
<a href="#">QUERY_STRING</a>	Information that follows the question mark (?) in the URL.
<a href="#">REMOTE_ADDR</a>	IP address of the client that made the request.
<a href="#">REMOTE_HOST</a>	Fully qualified domain name of the client that made the request.
<a href="#">REQUEST_METHOD</a>	HTTP request method.
<a href="#">SCRIPT_NAME</a>	Name of the script program being run.
<a href="#">SERVER_NAME</a>	Server host name or IP address.
<a href="#">SERVER_PORT</a>	TCP/IP port on which the request was received.
<a href="#">SERVER_PROTOCOL</a>	Name and version of the information retrieval protocol that relates to a request.
<a href="#">SERVER_SOFTWARE</a>	Name and version of the web server.
<a href="#">URL_PROTOCOL</a>	Default URL protocol (http or https).

**Tip:** You can use [TIBCO WebFOCUS Script Commands](#) on page 710 with HTTP header variables to further customize processing and control of the WebFOCUS Client.

This topic provides recommendations, information, and configuration steps for WebFOCUS 8 to meet the Payment Card Industry Data Security Standards that are outlined in the PCI DSS Version 3.0 document. This document is located at:

<https://www.pcisecuritystandards.org>

Customers can use this information to implement the required steps for PCI compliance.

We are committed to work in partnership with our customers, to further develop the standards in anticipation of future releases of WebFOCUS and changes in the PCI Security Standards.

**In this appendix:**

- ☐ [About the PCI Security Standards](#)
  - ☐ [Build and Maintain a Secure Network and Systems](#)
  - ☐ [Protect Cardholder Data](#)
  - ☐ [Maintain a Vulnerability Management Program](#)
  - ☐ [Implement Strong Access Control Measures](#)
  - ☐ [Regularly Monitor and Test Networks](#)
  - ☐ [Maintain an Information Security Policy](#)
- 

### About the PCI Security Standards

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security, and to facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements that are designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing. This includes merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks. The twelve requirements and subrequirements for PCI DSS compliance apply to all system components around technology and security, particularly that of the protection of cardholder data.

Based on an independent assessment by an information security company, and through an extensive evaluation process by the Qualified Security Assessor (QSA), WebFOCUS was evaluated in regard to Payment Card Industry Data Security Standard (PCI DSS) configuration best practices that are applicable to business intelligence functionality.

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Recommendations and Information for Requirement 1

- ❑ Install the WebFOCUS Client and the WebFOCUS Reporting Server on an internal (trusted) network segment, unexposed to the Internet Demilitarized Zone (DMZ).
- ❑ TCP/IP listener ports are required for certain WebFOCUS functionality. WebFOCUS also communicates to other non-WebFOCUS servers over TCP/IP, requiring access to those ports.

WebFOCUS TCP/IP Listener Ports

Default TCP/IP Ports	Usage	Remarks
WebFOCUS Reporting Server TCP/IP Listener Ports		
8120	TCP/IP listener	Should only be accessible from the WebFOCUS Client and the ReportCaster Distribution Server.
8121	HTTP or HTTPS listener	Should only be accessible from the internal (trusted) network.
8122	FOCUS listener	Can be disabled if not accessing multi-user FOCUS data sources.
8123	Java Services (JSCOM3) listener	Additional JSCOM3 listeners will require port numbers that increase by one (8124- <i>nnnn</i> ).
WebFOCUS Client		
1527	Relational database	Apache™ Derby, by default, but other relational databases can be used.

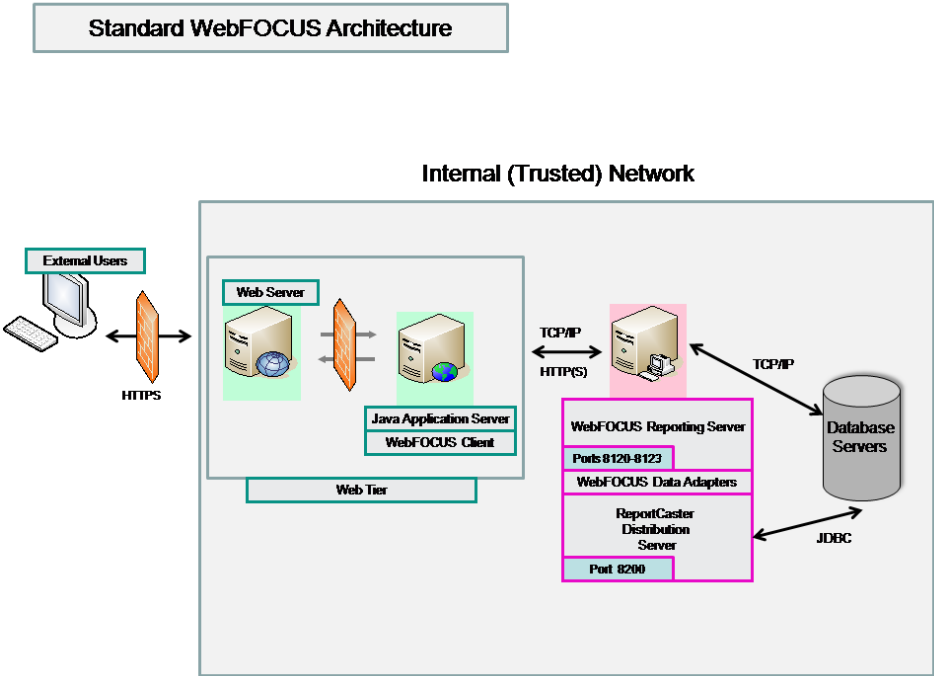
Default TCP/IP Ports	Usage	Remarks
<b>ReportCaster TCP/IP Ports</b>		
8200	Main listener	Should be accessible from the WebFOCUS Client.

**Access Required to Non-WebFOCUS TCP/IP and HTTP Ports**

Default TCP/IP Ports	Usage	Remarks
<b>WebFOCUS Reporting Server Access to TCP/IP Ports</b>		
Site dependent	Data adapters	Used for native and JDBC connections to database servers.
Site dependent	Adapter for Web Services	May need access to the HTTP port.
Site dependent	WebFOCUS Graphics, XLSX, Magnify and SOLR for indexing requests	Need access to the HTTP port. If using SSL, or any type of single sign on, JSCOM3 needs to be used.
389	LDAP server	Used for LDAP communication.
636	LDAP server	Used for LDAP communication over TLS/SSL.
<b>ReportCaster Access to TCP/IP Ports</b>		
25	Email server	Used for SMTP connections.
Site dependent	JDBC access to database server	Used for access to the Repository.
389	LDAP server	Used for LDAP communication.

Default TCP/IP Ports	Usage	Remarks
636	LDAP server	Used for LDAP communication over TLS/SSL.

The following image illustrates a standard WebFOCUS architecture model, and use of TCP/IP listener ports.



Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Recommendations and Information for Requirement Section 2.1

- ❑ Change the default WebFOCUS Managed Reporting administration credentials.

**Note:** Typically within a production environment, Administration Console access will be disabled, as configuration settings would not be altered.

- ❑ If installing Apache Tomcat™ from the WebFOCUS media, change the Tomcat administration credentials.

- ☐ Review and apply, where appropriate, security settings described in the *TIBCO WebFOCUS® Security and Administration Best Practices* documentation.

#### **Recommendations and Information for Requirement Section 2.2.1**

- ☐ Install WebFOCUS in at least a three-tier architecture, where the WebFOCUS Client is installed on one machine, the ReportCaster Distribution Server and the WebFOCUS Reporting Server are installed on a second machine, and the Database Servers are installed on separate machines.
- ☐ Firewall rules can be established based on information from Requirement 1. The WebFOCUS Reporting Server configuration parameter RESTRICT\_TO\_IP can be used to restrict access to the TCP/IP and HTTP listeners.

#### **Recommendations and Information for Requirement Sections 2.2.2 and 2.2.3**

- ☐ Configure the WebFOCUS Client and the WebFOCUS Reporting Server with the SSL protocol to provide secure HTTPS communication. For more information, see the related topics in this appendix and the *TIBCO WebFOCUS® Reporting Server Administration* manual.

#### **Recommendations and Information for Requirement Section 2.2.4**

Do not install any additional software or functionality that is not required by WebFOCUS.

- ☐ Minimally, WebFOCUS Client requires:
  - ☐ Java Application Server and Java Virtual Machine
  - ☐ Relational Database Management System
- ☐ WebFOCUS Reporting Server requires:
  - ☐ Database drivers for database access
  - ☐ Java Virtual Machine
- ☐ ReportCaster requires:
  - ☐ Java Virtual Machine

#### **Recommendations and Information for Requirement Section 2.3**

- ☐ The WebFOCUS Reporting Server browser interface can be configured for HTTPS. For configuration information, see the *TIBCO WebFOCUS® Reporting Server* manual.
- ☐ Communication to the WebFOCUS Client should use SSL to access the web server or application server infrastructure.

## Protect Cardholder Data

### Requirement 3: Protect stored cardholder data

#### Recommendations and Information for Requirement Section 3.3

- ☐ WebFOCUS developers must ensure that reports written in the TIBCO FOCUS language appropriately mask sensitive data.
- ☐ The Master File attribute, ACCESS=INTERNAL, should be added to hide columns that contain sensitive data.

#### Recommendations and Information for Requirement Section 3.4

- ☐ Limit creation of WebFOCUS extract files containing sensitive data.
- ☐ Traces should be enabled only for purposes of troubleshooting and gathering diagnostics, and preferably in a non-production WebFOCUS environment. Trace files should be purged immediately after use.
- ☐ Disable WebFOCUS Redirection for report output types, such as Excel® and PDF output.

### Requirement 4: Encrypt transmission of cardholder data across open, public networks

#### Recommendations and Information for Requirement 4

- ☐ If distributing content over public networks using FTP, ReportCaster must be configured to use SFTP.
- ☐ Configure the WebFOCUS Client to use AES128 or AES256 encryption for communication with the WebFOCUS Reporting Server, using a symmetric key negotiated through RSA PKI. For more information on configuring and implementing encrypted communication to the WebFOCUS Reporting Server, see [TIBCO WebFOCUS Encryption Features](#) on page 481.

## Maintain a Vulnerability Management Program

### Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

#### Recommendations and Information for Requirement 5

Requirements are not applicable to WebFOCUS.



## Requirement 6: Develop and maintain secure systems and applications

### Recommendations and Information for Requirement 6

- ☐ Ensure that the latest WebFOCUS service packs and hotfixes are applied. Refer to <http://techsupport.ibi.com> for the latest service packs and patches.
- ☐ Third-party software provided with the product, such as Tomcat and Java, should be updated as recommended by those vendors.

### Recommendations and Information for Requirement Section 6.3

- ☐ Adhere to internal Software Development Life Cycle (SDLC) recommendations for application development to ensure that any customizations do not introduce new vulnerabilities.
- ☐ Remove any test accounts created during development prior to a production rollout.

### Recommendations and Information for Requirement Section 6.4

- ☐ Create separate WebFOCUS environments for development, test, and production.
- ☐ WebFOCUS applications should not be developed directly on production environments.
- ☐ WebFOCUS Client and WebFOCUS Reporting Server service pack installations can be rolled back. For uninstall instructions, see the *TIBCO WebFOCUS® Installation and Configuration* manual for your platform.
- ☐ Change management provides the ability to move content from one environment to another.

### Recommendations and Information for Requirement Sections 6.5 and 6.6

- ☐ Use WebFOCUS Information Assurance best practices and coding techniques to eliminate application vulnerabilities. For information on all security settings that can be applied to public-facing web applications, see the *TIBCO WebFOCUS® Security and Administration Best Practices* documentation.
- ☐ For WebFOCUS applications that are public facing, customers must perform regular web application vulnerability assessments and/or install external firewalls.
- ☐ We adhere to established Software Development Life Cycle standards, when developing the WebFOCUS product, and has achieved an OWASP Application Security Verification Standard (ASVS) Level 3. Additional information is described in the *TIBCO WebFOCUS® Security and Administration Best Practices* documentation.

## Implement Strong Access Control Measures

### Requirement 7: Restrict access to cardholder data by business need to know

#### Recommendations and Information for Requirement 7

- ❑ WebFOCUS Managed Reporting and Business Intelligence Portal provide role-based security, along with optional privileges that should be used for access control.
- ❑ User access control, using Managed Reporting role-based security, can be integrated with the WebFOCUS Reporting Server using a shared authentication scheme. For more information, see [Authentication and Authorization](#) on page 217.
- ❑ Row-level and column-level security may be included, as needed, within WebFOCUS. For more information, see *Technical Memo 4694: WebFOCUS Row-Level and Column-Level Security*.

### Requirement 8: Identify and authenticate access to system components

#### Recommendations and Information for Requirement 8

- ❑ WebFOCUS should be configured to restrict multiple sign-ins by the same user. This can be done by clearing the Multiple Sign-ins Per User check box (False) on the Advanced page of the Administration Console Security tab.
- ❑ Passwords for WebFOCUS Managed Reporting users are stored in an SHA-512 iterative salted hash.
- ❑ Passwords for WebFOCUS service accounts are encrypted when stored using AES128 through AES256 encryption, using an internally or externally provided key.
- ❑ Passwords stored for service accounts for the WebFOCUS Reporting Server are encrypted using AES128 through AES256 encryption.
- ❑ WebFOCUS exits can be used for custom encryption, if the default methods are not sufficient. For more information, see [TIBCO WebFOCUS Encryption Features](#) on page 481.

- ☐ PCI DSS password policies can be implemented in the following ways:
  - ☐ Enabling Account Policies within the Administration Console.
  - ☐ WebFOCUS can be configured to delegate security to third-party authentication providers, such as Microsoft Active Directory, LDAP, Tivoli Access Manager, CA SiteMinder, and others.
- ☐ Public user access to cardholder data should be restricted.
- ☐ WebFOCUS can be configured to control session timeouts, which limit the amount of time users can remain active when using the following components:
  - ☐ Global.
    - ☐ Update the `drive:\ibi\WebFOCUS82\webapps\webfocus\WEB-INF\web.xml` file as follows:

```
<session-config>
<session-timeout>15</session-timeout>
</session-config>
```
- ☐ WebFOCUS applications authenticate all access to databases, using the following mechanisms:
  - ☐ Password Pass-through
  - ☐ Explicit
  - ☐ Trusted
- ☐ For ad hoc reporting and shared reports, customers must ensure that the appropriate controls and approvals are in place.

## Requirement 9: Restrict physical access to cardholder data

Requirements are not applicable to WebFOCUS.

## Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Recommendations and Information for Requirement 10

- ☐ The WebFOCUS Resource Analyzer can be used to audit and monitor application usage, including:
  - ☐ Procedure name, date-time started, execution time, CPU time used, wait time
  - ☐ Input and output operations, number of records, number of transactions, number of lines
  - ☐ MR Workspace, MR User, connection user ID, APP PATH, network connection
  - ☐ Selection criteria, data source, field
- ☐ The Resource Analyzer repository should be restricted to user IDs with proper authorization. For more information, see the *TIBCO WebFOCUS® Resource Analyzer Administrator's and User's Manual*.
- ☐ WebFOCUS logging is initialized when the application starts and remains active, as long as the application is running.
- ☐ Compensating controls for auditing user and administrative actions are provided.
- ☐ User access and administrative auditing are built into the product.

TIBCO WebFOCUS Logs

Log File	Usage	Remarks
WebFOCUS Managed Reporting		
audit.log	Tracks all sign-in changes and security-related changes.	For more information, see <a href="#">Logging</a> on page 591.
WebFOCUS Reporting Server		
edaprint.log	Tracks user connections	Connections made from the WebFOCUS Client and ReportCaster to the WebFOCUS Reporting Server.

## Requirement 11: Regularly test security systems and processes

### Recommendations and Information for Requirement Section 11.3

WebFOCUS software has been enhanced with a number of new security capabilities that emphasize strategic risk management and defend against malicious hacker attacks. This level of security is critical for external-facing, web-based business intelligence applications. WebFOCUS 8 software has achieved Level 3 Application Security Verification Standards low risk security certification against the most important security vulnerabilities and threats, as defined by the Open Web Application Security Project (OWASP).

Security defenses in the product include:

- ☐ XSS (Cross Site Scripting) defenses, to guard against XSS vulnerabilities.
- ☐ Session fixation defenses, to guard against session fixation vulnerabilities.
- ☐ CSRF (Cross Site Request Forgery) filter, to guard against CSRF vulnerabilities.
- ☐ Null byte injection filter, to guard against null injection vulnerabilities.
- ☐ Clickjacking filter, to guard against frame injection vulnerabilities.

For more information about Information Assurance and OWASP, visit <http://www.owasp.org>.

### Recommendations and Information for Requirement Section 11.5

For each component, directories containing critical WebFOCUS configurations are listed below, where *drive* refers to the WebFOCUS installation directory.

#### TIBCO WebFOCUS Configuration Directories

Directory	Usage	Remarks
<b>WebFOCUS Reporting Server</b>		
<i>drive</i> :\ibi\svr82\wfs\etc	TCP/IP communication and profiles	Used to define TCP/IP listener ports. Host global profile.
<i>drive</i> :\ibi\profiles	Profile information	Host and user profiles.
<i>drive</i> :\ibi\svr82\wfs\bin	edaserve.cfg	Main Reporting Server configuration file.

Directory	Usage	Remarks
<b>ReportCaster</b>		
<i>drive:\ibi\WebFOCUS82\ReportCaster\cfg</i>	Configuration information	Used to configure ReportCaster.  Files in this folder supplement the ReportCaster configuration file, dserver.xml, stored in the repository.
<b>WebFOCUS Client</b>		
<i>drive:\ibi\WebFOCUS82\client\wfc\web\cgi</i>	Trace information	Used to define trace levels.
<i>drive:\ibi\WebFOCUS82\client\wfc\etc</i>	Configuration information	Used to configure security, timeouts, and other configuration parameters.
<i>drive:\ibi\WebFOCUS82\config</i>	Configuration information	Used to configure security, timeouts, and other configuration parameters.
<i>drive:\ibi\WebFOCUS82\webapps</i>	Web applications	Used to host web applications packaged with WebFOCUS.

## Maintain an Information Security Policy

### Requirement 12: Maintain a policy that addresses information security for all personnel

Requirements are not applicable to WebFOCUS.

## Replicating the TIBCO WebFOCUS Repository Database

---

The Repository Database Replication utility transfers a copy of the WebFOCUS Repository from a source database to a target database. Because the utility preserves the integrity of the Repository database structure and contents during the transfer, you can use it to replicate the WebFOCUS Repository from Derby™ to Oracle®, Db2®, PostgreSQL®, MySQL AB®, or Microsoft SQL Server®.

### In this appendix:

- ☐ [Overview](#)
  - ☐ [Understanding Database Replication Settings](#)
- 

## Overview

Follow these steps to replicate the Repository database:

1. Create a target relational database.
2. Identify source and target database connection information and credentials.
3. Assign source and target database credentials and connection information to the appropriate settings in the Database Replication Settings file.
4. Run the Database Replication Utility.
5. Review the results of the replication utility run.
6. Replace the settings for the default WebFOCUS Repository database in the install.cfg file with those that identify the replicated WebFOCUS Repository database.
7. Test the connection to the replicated WebFOCUS Repository database.

For more information about the credentials and source and target database connection information you need in order to run the utility successfully, see [Understanding Database Replication Settings](#) on page 746.

As stated in the introduction, you can use this utility to replicate the Repository database from Derby to Oracle, Db2, PostgreSQL, MySQL AB, or Microsoft SQL Server. You can also use it to replicate the Repository database from these relational database management systems to Derby.

Please consult the Customer Support Team if you must replicate the Repository to any other database platform. The database replication utility cannot replicate the Repository to any non-relational database or to any database platform that does not use a JDBC driver.

**Procedure: How to Identify Source and Target Database Connection Information and Credentials**

To identify source database connection information and credentials, open the `utiluservars.bat` file and the `install.cfg` source files as described in the following steps.

1. Open the `utiluservars` file as follows:

- ❑ Windows: Navigate to `drive:\ibi\WebFOCUS82\utilities\setenv`, and open the `utiluservars.bat` file with a text editor.
- ❑ UNIX or Linux: Navigate to `install_directory/ibi/WebFOCUS82/utilities/setenv`, and open the `utiluservars.sh` file with a text editor.

The value in the `JDBC_PATH` parameter in this file is used as the value for the `SOURCE_JDBC_PATH` parameter in the `db_replication_settings` file.

2. Open the `install.cfg` file as follows:

- ❑ Windows: Navigate to `drive:\ibi\WebFOCUS82\config` and open the `install.cfg` file with a text editor.
- ❑ UNIX or Linux: Navigate to `install_directory/ibi/WebFOCUS82/config` and open the `install.cfg` file with a text editor.

The values in the `IBI_REPOS_DB_URL`, `IBI_REPOS_DB_DRIVER`, and `IBI_REPOS_DB_USER` parameters in this file are used as the values for the `SOURCE_REPOS_DB_URL`, `SOURCE_REPOS_DB_DRIVER`, and `SOURCE_USER_NAME` parameters in the `db_replication_settings` file.

3. Keep both files open until the configuration of the Database Replication Settings file is complete.
4. To identify target database connection information and credentials, contact the database administrator who created the empty target database.

Or

Review the target database configuration and documentation provided by the vendor.

The location and configuration of the specific values in the target database vary by vendor and are beyond the scope of this document.



**Procedure: How to Prepare the Database Replication Settings File**

Before you begin, ensure that an empty relational database was created to serve as the target database, and that the most current database credentials and connection information are available for the source database and the target database.

1. Open the `db_replicate_settings` file as follows:
  - ❑ For Windows: Navigate to `drive:\ibi\WebFOCUS82\utilities\dbupdate`, and open the `db_replicate_settings.bat` file with a text editor.
  - ❑ For UNIX or Linux: Navigate to `install_directory/ibi/WebFOCUS82/utilities/dbupdate`, and open the `db_replicate_settings.sh` file with a text editor.
  - ❑ **Note:** If you want to keep a backup copy of the original version of the `db_replicate_settings` file, create a copy of the file you are updating before making changes.
2. Scroll down to the source section of the file.
3. In the `SOURCE_CLASS_PATH` parameter, accept the pathname displayed, by default, without making any changes.
4. In the `SOURCE_JDBC_PATH` parameter, replace the sample value with the pathname to the source database JDBC driver, as identified in the `JDBC_PATH` parameter of the `utilusersvars.bat` file.

This value must be enclosed in quotation marks ("").

5. In the `SOURCE_REPOS_DB_URL` parameter, replace the sample value with the URL from the `IBI_REPOS_DB_URL` parameter of the `install.cfg` file.
6. In the `SOURCE_REPOS_DB_DRIVER` parameter, replace the sample value with the JDBC driver class name from the `IBI_REPOS_DB_DRIVER` parameter of the `install.cfg` file.
7. In the `SOURCE_USER_NAME` parameter, replace the user ID from the `IBI_REPOS_DB_USER` parameter of the `install.cfg` file.

Make sure that the characters and format of the user ID are an exact match to the user ID as it appears in the source database and that there are no excess spaces before or after the user ID.

If you do not assign a valid user ID to this parameter, the database replication utility prompts you for it at run time.

8. In the `db_replicate_settings` file `SOURCE_PASSWORD` parameter, type the password assigned to the Repository user name during the product installation.

This value is encrypted in the `IBI_REPOS_DB_PASSWORD` parameter in the `install.cfg` file, so you cannot paste it from the `install.cfg` file.

Make sure that the characters and format of the password are an exact match to the password as it appears in the source database and that there are no excess spaces before or after the password.

If you do not assign a valid password to this parameter, the database replication utility prompts you for it at run time.

9. Scroll down to the target section of the file.
10. In the TARGET\_JDBC\_PATH parameter, type over the sample value with the pathname to the JDBC driver of the target database.

If your JDBC driver consists of more than one jar file, separate multiple jar file paths with a semi-colon.

11. In the TARGET\_REPOS\_DB\_URL parameter, type over the sample value with the URL of the target database connection.
12. In the TARGET\_REPOS\_DB\_DRIVER parameter, type over the sample value with the class name of the target database JDBC driver.
13. In the Å\_NAME parameter, type the user ID assigned to the new database when it was created.

Make sure that the characters and format of the user ID are an exact match to the user ID as it appears in the target database and that there are no excess spaces before or after the user ID.

If you do not assign a value user ID to this parameter, the database replication utility prompts you for it at run time.

14. In the TARGET\_PASSWORD parameter, type the password assigned to the new database user ID.

Make sure that the characters and format of the password are an exact match to the password as it appears in the target database and that there are no excess spaces before or after the password.

If you do not assign a valid password to this parameter, the database replication utility prompts you for it at run time.

15. Save and close the db\_replicate\_settings file with your changes.

**Procedure: How to Run the Database Replication Utility**

Before you begin, ensure that a target database is available in an accessible location, and that you have assigned source and target database user credentials and connection information to the `db_replicate_settings` files.

1. Start the database replication utility as follows:
  - ❑ For Windows: Navigate to `drive:/ibi/WebFOCUS82/utilities/dbupdate`, and double-click `db_replicate.bat`.
  - ❑ For UNIX or Linux: Navigate to `install_directory/ibi/WebFOCUS82/utilities/dbupdate`, and double-click `db_replicate.sh`.
2. If you receive one of the following prompts, respond as directed in the following substeps, and press the Enter key after each response:
  - a. Enter Source Database Repository Username: Type the user ID assigned to the WebFOCUS Repository created during the product installation.
  - b. Enter Source Database Repository password: Type the password assigned to the Repository user name.
 

**Note:** When you type this value, the cursor remains in place and does not show any typed characters.
  - c. Enter Target Database Repository Username: Type the user ID assigned to the new database when it was created.
  - d. Enter Target Repository Database Password: Type the password assigned to the new database user ID.
 

**Note:** When you type this value, the cursor remains in place and does not show any typed characters.
3. Monitor the Command Prompt window while it displays a list of the parameters and values provided for this run of the utility.
4. When you receive a message stating that the DB update process is starting, wait while the utility completes the database replication process. This could take several seconds.
5. If you receive an error message that stops the utility, such as jdbc driver not found, credentials invalid, or credentials don't have ability to access source or target:
  - a. Close the Command Prompt window.
  - b. Revise the values assigned to the `db_replicate_settings` file, as described in [How to Prepare the Database Replication Settings File](#) on page 741.

You can also review these errors in the `db_replicate_install` log file created for this run of the utility. For more information on how to open and review the log file, see [How to Review the Results of the Replication](#) on page 744.

6. When you receive a message stating that the database update was successful, press any key to close the Command Prompt window.

**Procedure: How to Review the Results of the Replication**

You can use database replication utility logs to identify and address any errors that occurred during the replication process. Logs generated by the utility are located in the `application_logs` directory in Release 8.2 Version 05 and higher.

1. Sign in as an administrator, and open the Administration Console.
2. Click the *Diagnostic* tab, and then click *Application Log Files*.
3. On the Application Log Files page, click `db_replicate_install_2_YYYY-MM-DD_HH-MM-SS.txt`, where YYYY-MM-DD\_HH-MM-SS represents the date and time the database replication utility log file was created.
4. Review records in the log file page to ensure that the replication is complete, and that no error messages preventing it from completing successfully are present.

If the final entry reads, Update process SUCCEEDED, the replication completed successfully.

5. Close the log file page, and sign out.

**Procedure: How to Redirect the Repository Database From the Old Source Database to the New Target Database**

If the source database remains the principal Repository database after the replication, no further review or updates are necessary. However, if the target database becomes the new principal Repository database, you must also complete the activation of the newly-replicated Repository database by opening the `install.cfg` file and replacing the user name, password, database driver, and database URL of the source database with those of the target database.

1. Stop the Application Server, if it is running.
2. Navigate to the `config` directory.
  - ❑ On Windows: `drive:\ibi\WebFOCUS82\config`
  - ❑ On Unix or Linux: `install_directory/ibi/WebFOCUS82/config`
3. Create and save a backup copy of the `install.cfg` file.
4. Open the `install.cfg` file in a text editor.
5. In the `IBI_REPOS_DB_USER` parameter, type over the existing value from the source database with the user name assigned to the target database.

Make sure that the characters and format of the user ID are an exact match to the user ID as it appears in the source database and that there are no excess spaces before or after the user ID.

6. In the IBI\_REPOS\_DB\_PASSWORD parameter, type over the encrypted password from the source database with the new plain text password assigned to the database user in the target database.

Make sure that the characters and format of the password are an exact match to the password as it appears in the source database and that there are no excess spaces before or after the password.

The plain text password is encrypted automatically when you restart the Application Server.

7. In the IBI\_REPOS\_DB\_DRIVER parameter, type over the class name of the database driver of the source database with the class name of the database driver of the target database.
8. In the IBI\_REPOS\_DB\_URL parameter, type over the URL for the source database connection with the URL for the target database connection.
9. Confirm that the new values are correct, and then save and close the install.cfg file.
10. Re-start the Application Server to encrypt the plain text Repository Database User password in the install.cfg file.

**Note:** During the restart, the Application Server will attempt to utilize the new RDBMS.

### **Procedure:** How to Test the New Repository Database Connection

1. If the Application Server was not stopped and restarted after updating the install.cfg file, start or restart it before you begin.
2. Sign in as an administrator and open the Administration Console.
3. Open the Database Replication Utility Log File, as described in [How to Review the Results of the Replication](#) on page 744.
4. Review the log file for error messages.
5. Address any errors that occurred when the Application Server attempted to connect to the new RDBMS.
6. When you have addressed errors in the Database Replication Utility log file, sign in again as an administrator.
7. If you encounter errors during sign in, review the values assigned to the IBI\_REPOS\_DB settings in the install.cfg file to ensure they contain the appropriate connection values for the new target database.
8. If you are able to run the report with no errors, you have successfully established a connection to the target database.

## Understanding Database Replication Settings

Values for the settings required by the database replication utility are stored in the `db_replicate_settings` file. This file contains four main sections: Prompt if Needed, Samples, Source, and Target.

The Prompt if Needed section enables you to activate or deactivate the interactive mode for the Database Replication Utility. This mode is activated, by default, ensuring that you are prompted to add missing database connection information whenever you run the database replication utility.

The Samples section contains sample Database Driver paths, Database Driver URLs, and sample JDBC Paths for various RDBMS providers, including MS SQL Server®, PostgreSQL, MySQL™, Db2®, Oracle®, and Derby™. Consult the latest version of the `db_replicate_settings` file for full details.

The Source section contains the following settings that define connection information for the Repository database created during the product installation. This database serves as the source of the replication.

With the exception of the `SOURCE_CLASS_PATH` value, you must replace the sample values in the Source section with those that conform to the values used in your local installation of WebFOCUS if your local configuration does not match the sample values assigned to the settings in the `SOURCE` section. You can clear these values if you prefer to have the Database Replication Utility prompt you for this information at run time.

**❑ `SOURCE_CLASS_PATH`.** Defines the location of the entity classes matching the database that is to be replicated. The `CLASSPATH` is the location of the `IBFSCCommands.jar` file for the WebFOCUS Repository. The value in this setting must not be updated.

The database replication utility does not define a classpath for the target database.

In the `db_replicate_settings` file, the value assigned to this setting contains the variable `%WFROOT%` for the Windows version or `${WFROOT}` for the UNIX version. This variable captures the root directory for your installation of WebFOCUS. Within that root directory, the location of the `IBFSCCommands.jar` file remains the same:

- ❑ For Windows: `\utilities\lib\`
- ❑ For UNIX or Linux: `/utilities/lib/`

**❑ `SOURCE_JDBC_PATH`.** Defines the full path to the location of the jar files that make up the JDBC driver for the source database. If the JDBC driver consists of more than one jar file, multiple jar file paths are separated with a semicolon (;).

You must replace the sample value assigned to this field with the pathname used by your organization before running the database replication utility.

You can identify the location of the source database JDBC driver in use in your installation of WebFOCUS in the JDBC\_PATH parameter of the utiluservars.bat file, which is located in *drive:\ibi\WebFOCUS82\utilities\setenv* for Windows, or *install\_directory/ibi/WebFOCUS82/utilities/setenv* for UNIX or Linux.

- ❑ In most Windows-based installations of WebFOCUS, the JDBC driver jar files are stored in the location, *drive:\ibi\derby\lib\derbyclient.jar*.
- ❑ In most Unix or Linux-based installations of WebFOCUS, the JDBC driver jar files are stored in the location, *install\_directory/ibi/Drivers/derbyclient-10.8.1.2.jar*.
- ❑ **SOURCE\_REPOS\_DB\_URL.** Defines the URL that identifies the connection string to the source database. This URL takes the form:

*jdbc:subprotocol:node/databaseName*

where:

*jdbc*

Is the java database class protocol.

*subprotocol*

Is the protocol for the RDBMS that hosts the database. For example, *derby//localhost*.

**Note:** If the database resides on the same computer node as the java program, the hostname part and the corresponding double slashes of the *jdbc* can be skipped. For example, *jdbc:odbc:wham*.

*node*

Is the number of the port on the machine that hosts the database. For example, 8080, if the database is on the same machine.

*databaseName*

Is the name of the Repository database or its copy. For example, WebFOCUS82.

You must replace the sample value assigned to this field with the database connection string used by your organization before running the database replication utility.

You can identify the source database URL in use in your installation of WebFOCUS in the IBI\_REPOS\_DB\_URL parameter of the install.cfg file, which is located in *drive:\ibi\WebFOCUS82\config* for Windows, or *install\_directory/ibi/WebFOCUS82/config* for UNIX or Linux.

In most Windows-based and UNIX or Linux-based installations of WebFOCUS, the database connection string is:

```
jdbc:derby://localhost:1527/WebFOCUS82;
```

- ❑ **SOURCE\_REPOS\_DB\_DRIVER.** Defines the location of the jar file that contains the Java Database Connectivity (JDBC) driver for the Repository, which is the source database. The JDBC driver class provides network connectivity to the Network Server for this database.

You can identify the URL in use in your product installation in the IBI\_REPOS\_DB\_DRIVER parameter of the install.cfg file, which is located in *drive:\ibi\WebFOCUS82\config* for Windows, or *install\_directory/ibi/WebFOCUS82/config* for UNIX or Linux.

In most product installations, the location of the jar file that contains the Java Database Connectivity (JDBC) driver is:

```
org.apache.derby.jdbc.ClientDriver
```

- ❑ **SOURCE\_USER\_NAME.** Defines the ID for the source database user. When you run the utility, this setting should contain the user name assigned to the Repository during product installation.

You can identify the user ID of the source database in use in your product installation in the IBI\_REPOS\_DB\_USER parameter of the install.cfg, which is located in *drive:\ibi\WebFOCUS82\config*, for Windows or *install\_directory/ibi/WebFOCUS82/config* for UNIX or Linux.

This setting contains the sample value `username`, by default. If you run the Database Replication Utility without specifying the source database user ID in this field, you are prompted to type the source database user name.

A database user ID grants access to information and resources in the database to the users and applications to which it is assigned. The user ID for the source database must have the right to read database objects.

- ❑ **SOURCE\_PASSWORD.** Defines the password assigned to the source database user. When you run the utility, this setting should contain the password assigned to the Repository during product installation.

An encrypted version of the password assigned to the source database user in use in your product installation appears in the IBI\_REPOS\_DB\_PASSWORD parameter of the install.cfg file, which is located in *drive:\ibi\WebFOCUS82\config* for Windows, or *install\_directory/ibi/WebFOCUS82/config* for UNIX or Linux.



This setting contains the sample value password, by default. If you run the Database Replication Utility without specifying the source database password in this field, you are prompted to type the password for the source database user.

This password for the source database authenticates the identity of the source database User ID.

The TARGET section of the Database Replication Settings file contains the following settings that define the connection for the database targeted by the replication.

You must always replace the sample values in the TARGET section with those that conform to the target database you wish to create, or clear those values if you prefer to have the Database Replication Utility prompt you for this information at run time.

- ❑ **TARGET\_JDBC\_PATH.** Identifies the location of the jar file that contains the Java Database Connectivity (JDBC) driver for the target database. The JDBC driver class provides network connectivity to the Network Server for the target database.

You must replace the sample value with the target database JDBC Path before running the database replication utility.

- ❑ **TARGET\_REPOS\_DB\_URL.** The URL that identifies the connection string to the target database. This URL takes the form:

*jdbc:subprotocol:node/databaseName*

where:

*jdbc*

Is the java database class protocol.

*subprotocol*

Is the protocol for the RDBMS that hosts the database. For example, derby//localhost.

**Note:** If the database resides on the same computer node as the java program, the hostname part and the corresponding double slashes of the jdbc can be skipped. For example, jdbc:odbc:wham.

*node*

Is the number of the port on the machine that hosts the database. For example, 8080, if the database is on the same machine.

*databaseName*

Is the name of the target database.

You must replace the sample value with the URL of the target database before running the Database Replication Utility.

- ❑ **TARGET\_REPOS\_DB\_DRIVER.** Defines the location of the jar file that contains the Java Database Connectivity (JDBC) driver for the target database. The JDBC driver class provides network connectivity to the Network Server for the target database.

You must replace the sample value with the location of the JDBC driver for the target database before running the Database Replication Utility.

- ❑ **TARGET\_USER\_NAME.** Defines the user ID for the target database. When you run the utility, this setting should contain the user name assigned to the target database when it was created.

However, it contains the sample value, `username`, by default. If you run the Database Replication Utility without specifying the target database user ID in this field, you will be prompted to type the target database user name.

A database User ID grants access to information and resources in the source database to the applications and the users to which it is assigned. The User ID for the target database must have the right to create and modify database objects.

- ❑ **TARGET\_PASSWORD.** Defines the password assigned to the target database user. When you run the utility, this setting should contain the password assigned to the target database user name during the creation of the target database.

However, it contains the sample value, `password`, by default. If you run the Database Replication Utility without specifying the target database password in this field, you are prompted to type the password for the target database user.

This password authenticates the identity of the Database User ID for the target database.

# Glossary

---

**Administration Console**

The interface that administrators use to manage the WebFOCUS environment and configuration settings.

**Administration privileges**

System administrator privileges that are generally only assigned to WebFOCUS administrators.

**Advanced Reporting privileges**

Privileges that can be assigned to users who need to create and share their own reports, generally granted as a supplement to the Basic Reporting privileges.

**alternate zone**

The security zones that defines secondary authentication methods to be used based on the user network location.

**anonymous access**

Unauthenticated access to resources.

**Application Development privileges**

Privileges that can be assigned to developers so they can create complete WebFOCUS applications using only web-based tools.

**auditing**

The process of tracking user access to tools and resources and logging important administrative actions.

**authentication**

The process of confirming the identity of a user.

**authorization**

The process of enforcing user privileges to control the access to resources and tools within an application.

**AUTOADD**

The process of automatically adding pre-authenticated and externally authenticated users to WebFOCUS, if the user accounts exist in the external source, but do not already exist in WebFOCUS.

<b>Basic Reporting privileges</b>	Privileges that can be assigned to most users, including those with minimal training. All of the other sets of privileges are granted in addition to the basic reporting features.
<b>Clear Inheritance</b>	Removes an inherited rule for a role on a resource, changing the access on the resource to Not Set. When a user belongs to multiple roles with overlapping privileges, any privileges shared with the cleared role will be evaluated to Not Set.
<b>clickjacking</b>	A web attack that nests content inside frames to trick users into clicking on a button or link and unknowingly enabling a malicious action. Clickjacking is also known as a UI redress attack.
<b>Cross-Site Request Forgery (CSRF)</b>	A web attack that injects malicious scripts into trusted web sites.
<b>default zone</b>	The security zone that defines the default form of authentication used. This zone determines that authentication method used for any request not processed by one of the other zones.
<b>Deny</b>	Disables a privilege.
<b>Desktop Development privileges</b>	Privileges that enable developers to use the Windows-based WebFOCUS desktop products.
<b>effective policy</b>	The result of all rules applied to the user for a given resource. This may be evaluated as permitted or denied.
<b>EVERYONE group</b>	The group of all users in the system. New users are assigned to this group, by default.

<b>explicit group</b>	A group in which a user has been directly placed.
<b>external authentication</b>	The process of confirming the identity of a user through an application other than WebFOCUS.
<b>folder</b>	A container for repository content.
<b>group</b>	A collection of users or subgroups which require similar capabilities or access to the same resources.
<b>Group Administration privileges</b>	Privileges that can be assigned to department or tenant group administrators so that they can manage their users and the content created by their users.
<b>hybrid privilege</b>	A privilege that is both a system privilege and a privilege for one or more subsystems. Hybrid privileges are used for multiple purposes, such as when a privilege enables access to an item in a toolbar menu and an item in a context menu.
<b>IBFS File System</b>	A logical addressing system used by WebFOCUS software to store and retrieve objects. Every object has a unique IBFS path.
<b>implicit group</b>	A group to which a user belongs by implication, without being a direct member. For example, users who explicitly belong to a subgroup or who are dynamically determined to be a member of a subgroup also implicitly belong to the parent of that group.
<b>Legacy privileges</b>	Privileges that enable legacy product behavior for customers migrating to WebFOCUS 8 from previous versions.

**Lightweight Directory  
Access Protocol (LDAP)**

An application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. WebFOCUS software can be configured to use LDAP for external authentication or authorization.

**local privilege**

A privilege that is applied to one or more subsystems and not also listed as a session privilege. Generally, local privileges enable or disable context menu items or tools. They are evaluated when the user interface is rendered.

**My Content**

The reports, output, and schedules created by a user.

**monitor ID**

A unique, randomly generated identifier for each client session. The monitor ID allows an administrator to reference sessions without exposing individual user application server session IDs.

**name**

The unique IBFS name of an object.

**Not Set**

Determines that a privilege is neither enabled nor disabled, which implicitly denies the privilege.

**order of precedence**

The order of operations that determines whether a privilege is permitted or denied for a user in a particular location.

**Over Permitted**

Overturns a denied rule for a specific location, permitting the privilege on that folder. The rule is still evaluated to Denied on the children of the folder, unless another rule applies.

<b>password complexity</b>	Determines password requirements, including length, whether the user account name or user name can appear in the password, and whether uppercase letters, lowercase letters, digits, and non-alphabetic characters are mandatory.
<b>Permit</b>	Enables a privilege.
<b>portlet zone</b>	The security zone that defines the authentication method for WebFOCUS Open Portal Services products, including SharePoint.
<b>pre-authentication</b>	A WebFOCUS authentication method that relies on authentication already performed by a third-party security provider.
<b>private resource</b>	Content that is available only to the owner and to authorized users with whom it is shared.
<b>privilege</b>	An atomic function that controls access to a tool, resource, or ability.
<b>PTH</b>	(Process Table Handler) The default security provider used when the WebFOCUS Reporting Server is first installed. Users are authenticated against a list maintained in the admin.cfg file.
<b>published resource</b>	Content whose availability is determined by rules, rather than the individual decision to share it. Published content is considered authoritative and has usually undergone quality assurance and testing before being published for the user community.
<b>Remember Me</b>	A feature that gives users the option of bypassing the Sign in page. This feature is not supported with pre-authentication methods.

<b>repository</b>	A relational database that contains all information about WebFOCUS resources.
<b>resource</b>	Any folder, item, library content, portal, privilege, report procedure, role, user, or group to which access can be controlled or to whom abilities can be granted.
<b>resource template</b>	A template that creates folders, rules, roles, and portals based on an existing model. For example, an enterprise domain template or a SaaS tenant domain template.
<b>resource tree</b>	A visual display of the servers, portals, content, and change management packages in the repository.
<b>reverse proxy server</b>	A web server that acts as an intermediary between an external network and the web server on which WebFOCUS software is installed.
<b>role</b>	A group of similar or useful bundled privileges.
<b>rule</b>	Determines the privileges to which a user has access for a given resource. Every rule must have a subject (user or group), a role, an action (such as permit or deny), and a scope.
<b>Scheduling and Distribution privileges</b>	Privileges that can be assigned to users, developers, and administrators so they can create schedules that distribute reports with ReportCaster.
<b>scope</b>	Controls whether a rule applies to a folder or to a folder and its children.



<b>Security Center</b>	The interface used to manage users, groups, roles, and rules. This management ability may be delegated to users or groups without full administrative control.
<b>security provider</b>	Authenticates and authorizes users.
<b>security token</b>	A type of two-factor authentication security device used to authorize the use of computer services.
<b>security zones</b>	Specify different authentication methods based on configurable criteria.
<b>service account</b>	An account used to execute services or perform system tasks that should not be performed by an individual user account.
<b>service provider</b>	In a SaaS deployment, the organization that implements WebFOCUS software and grants controlled access to its clients and tenant users.
<b>session privilege</b>	A privilege that is identified during the sign-in process and then cached for the duration of the session.
<b>shared resource</b>	A private resource that an individual user has shared with other users or groups. Shared resources are made available to users through the Shared Content folder.
<b>single sign on (SSO)</b>	Access to multiple related, but independent, software systems.

**Software as a Service (SaaS)**

A business model in which an organization provides controlled access to their services to multiple clients.

**subsystem**

A component in the hierarchy that organizes objects in the WebFOCUS Repository.

**superuser**

An account with the special privileges needed to administer and maintain the system. Superuser access overrides all other security rules.

**tenant**

In a SaaS deployment, a client organization which is granted controlled access by the client service organization that implements WebFOCUS software. In a multi-tenancy deployment, although tenant users belong to the EVERYONE group, along with the service provider users, the tenant users are only aware of other users within their own organization.

**title**

The display name of an object.

# Legal and Third-Party Notices

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE "LICENSE" FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document contains confidential information that is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of TIBCO Software Inc.

TIBCO, the TIBCO logo, the TIBCO O logo, FOCUS, iWay, Omni-Gen, Omni-HealthData, and WebFOCUS are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle Corporation and/or its affiliates.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

This software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the readme file for the availability of this software version on a specific operating system platform.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

---

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

This and other products of TIBCO Software Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (<https://www.tibco.com/patents>) for details.

Copyright © 2022. TIBCO Software Inc. All Rights Reserved. TIBCO Confidential Information.

# Index

(IBI\_AJAX\_TIMEOUT) [526](#)

&FOCSECUSER [212](#)

\$BOTTOM keyword [657](#)

## A

ACCESS attribute [654](#), [662](#), [670](#)

access control [18](#)

Access Control Templates [401](#)

access to data [653](#), [666](#)

    commands [663](#)

    restricting [653](#), [654](#), [666](#), [670](#)

Account Policies settings

    IBI\_Multiple\_Logins\_Per\_User [149](#)

administration [61](#), [725](#)

Administration Console [61](#), [98](#), [104](#)

    adding nodes to files [97](#)

    Client Settings [481](#)

    Client Verification [174](#)

    diagnostics menu [172](#)

    Multiple Reports settings [549](#)

    navigating [69](#)

    OLAP settings [550](#)

    Quick Data [565](#)

    Redirection Settings [481](#)

    traces [172](#)

    verification tools [174](#)

Administrators Group [458](#)

Advanced Settings [149](#)

    IBI\_User\_Namespace [151](#)

advanced users [366](#)

AES encryption provider [483](#)

agent behavior [27](#)

All Clients trace [631](#)

Allow Embedding [161](#)

altdnode.wfs configuration file [103](#)

Alternate Server Mapping [102](#)

alternate server nodes [103](#)

Anonymous access [227](#)

    enable [228](#)

Anonymous Group [458](#)

Anonymous User

    BI Portal Availability [231](#)

Apache Tomcat [223](#)

App Studio [19](#)

App Studio custom logon templates [689](#)

    authentication template [692](#), [697](#)

    cookie exclude list [698](#)

    how they work [689](#)

    logon resource [692](#)

    logon result [694](#)

    optional logon parameters [695](#)

    required logon parameters [694](#)

    tags [692](#)

    template file [697](#)

    variables [695](#)

Application Caches Settings [513](#)

Application Caches

IBI\_DATAVALUES\_CACHE\_GLOBALPATHS [515](#)

IBI\_DATAVALUES\_CACHE\_MAXMEG [518](#)

Application Contexts settings [519](#)

IBI\_Help\_Context [519](#)

IBI\_Help\_Proxy\_Context [520](#)

IBI\_Help\_Proxy\_Host [520](#)

IBI\_HELP\_PROXY\_SECURE [520](#)

IBI\_REPORT\_CACHE\_ENABLE [518](#)

IBI\_ReportCaster\_Context [521](#)

IBI\_Webapp\_Context\_Default [521](#)

IBI\_WEBAPP\_DEFAULT\_URL [521](#)

IBI\_WebFOCUS\_Context [521](#)

Application Directories settings [522](#)

IBI\_Approot\_Directory [522](#)

IBI\_Export\_Directory [522](#)

IBI\_Import\_Directory [522](#)

IBI\_Log\_Retain\_Days [522](#)

IBI\_Repository\_Root\_Directory [522](#)

IBI\_SCM\_Staging\_Directory [522](#)

IBI\_Temporary\_Directory [522](#)

IBI\_Trace\_Directory [522](#)

IBI\_Trace\_Retain\_Days [523](#)

Application Log [205](#)

Application Log Files Page [204](#)

application server [19](#)

attributes [653](#)

database security [653](#)

audit logs

accessing [593](#)

auditing [18](#), [593](#)

AUTH\_TYPE variable [725](#)

authentication [18](#), [218](#)

by Active Directory [321](#)

by LDAP [321](#)

external [321](#)

authorization [18](#)

external [326](#)

internal [326](#)

user [18](#)

Auto Describe [561](#)

## B

backslash escape character (\) [714](#)

basic cluster functionality [97](#)

Basic Portal

icon [232](#)

basic users [366](#)

BI (Business Intelligence) Portal [19](#)

BI Portal [19](#), [231](#)

IBI\_CONCURRENT\_PUBLIC\_SESSION\_LIMIT  
[526](#)

IBI\_DEFAULT\_WORKSPACE\_PATH [527](#)

IBI\_V3\_DEFAULT\_LAYOUT [532](#)

IBI\_V3\_PORTAL [532](#)

IBI\_V4\_PORTAL [532](#)

Business Intelligence (BI) Portal [19](#)

## C

cache clearing [87](#)

- CALL command [712](#)
- case sensitive passwords [660](#)
- Central Authentication Service (CAS) [234](#)
- Change Management [487](#)
  - Collaborative Portals [491](#)
  - creating packages [489](#)
  - Export Using the Command-Line Interface [500](#)
  - Import Using the Command-Line Interface [506](#)
  - moving application files [488](#)
- CHECK command [663](#)
- CHECK FILE command
  - DBA and [664](#)
- checking variables [721](#), [722](#)
- Clear Cache [87](#)
- Clear Inheritance [363](#)
- Client [19](#)
  - configuration files [511](#)
  - connections and permissions [174](#)
  - Connector Trace [631](#)
  - license management [81](#)
  - Reconnection to Repository [102](#)
- Cluster Manager [88](#), [104](#)
- clustered servers basic functionality [97](#)
- CNCTUSER [212](#)
- Collaborative Portal
  - Icon [232](#)
- COMBINE command and data security [676–678](#), [681](#), [682](#)
- commands [663](#)
  - user access levels [663](#)
- CONDITIONAL\_INCLUDE command [710](#), [711](#), [715](#)
- confidentiality [18](#)
- configuration events [603](#)
- configuration files [511](#), [709](#), [710](#)
  - altdnode.wfs [103](#)
  - odin.cfg [97](#)
- Configuration Tab [70](#)
- Configuring trusted connections [49](#)
- configuring
  - InfoAssist Basic [81](#)
  - InfoAssist for MR [81](#)
  - Magnify license [81](#)
  - Quick Data [81](#)
  - Server settings [97](#)
  - WebFOCUS Mobile [81](#)
- Constrained Delegation
  - Kerberos [257](#)
- content events [604](#)
- Content view [350](#)
- CONTENT\_LENGTH setting [725](#)
- CONTENT\_TYPE variable [725](#)
- CopyHTTPCookieToWFVar method [720](#)
- CopyHTTPHeaderToWFVar method [717](#)
- CopyHTTPMethodToWFVar method [720](#)
- CopySessionVarToWFVar method [719](#)
- CopyWFVarToSessionVar method [717](#)
- CORS [164](#), [165](#)
- CREATE command [663](#), [664](#)
- Cross-Origin Resource Sharing [164](#)
  - Allow Embedding [161](#)

Cross-Origin Resource Sharing [164](#)

    Allowing [165](#)

Cross-Origin Settings

    Configuring [159](#)

Custom Settings [124](#)

    Configuring [125](#)

Custom Single Sign On (SSO) Authentication [255](#)

custom variables [722](#), [723](#)

Custom Welcome Page

    Redirect /ibi\_apps to [524](#)

## D

data access [18](#), [653](#), [666](#)

    levels of [662](#), [666](#), [668](#)

    restricting [654](#), [670](#)

    security attributes [653](#)

data encryption [684](#), [685](#)

    performance considerations [685](#)

data integrity [18](#)

data security [536](#), [653–655](#)

    access levels [662](#), [666](#), [668](#)

    central Master File [676–678](#)

    CHECK FILE command and [664](#)

    COMBINE command and [676–678](#), [681](#), [682](#)

    encrypting Master Files [684](#)

    encrypting segments [684](#), [685](#)

    filters [682](#)

    JOIN command and [676–678](#), [681](#), [682](#)

    passwords [661](#)

    restricting access [668](#), [670](#), [671](#)

data security [536](#), [653–655](#)

    special considerations [656](#)

data source security [653](#)

data sources

    access control [653](#), [666](#)

    security [653–655](#)

database administration (DBA) [653](#)

    attributes [653](#)

    CHECK FILE command and [664](#)

    displaying decision tables [670](#)

database administration (DBA)security [653](#)

Database Administrators (DBAs) [654](#)

    identifying [654](#)

    security privileges [657](#)

DBA (database administration) [653](#)

    attributes [653](#)

    CHECK FILE command and [664](#)

    displaying decision tables [670](#)

    passwords [536](#)

DBA attributes [653](#)

DBA decision table [670](#)

DBA exit [709](#)

DBA passwords [657](#), [658](#)

DBA security [657](#)

    HOLD files [657](#)

DBACSENSITIV parameter [660](#)

DBAFILE attribute [676–678](#)

    file naming requirements [681](#)

DBAJoin [676](#)



DBAs (Database Administrators) [654](#)

identifying [654](#)

security privileges [657](#)

DBATABLE [670](#)

DBATABLE procedure [670](#)

decision tables [670](#)

DECRYPT command [663](#), [664](#)

decrypting procedures [687](#)

Default Autoprompt Template [561](#)

deferred receipt security [213](#)

Deferred Reporting settings

IBI\_Deferred\_Custom\_Description [542](#)

IBI\_Deferred\_Notify\_Submitted [542](#)

IBI\_Deferred\_Ticket\_Delete\_Confirm [542](#)

DEFINE command [663](#), [664](#)

deployment options [17](#), [20](#), [23](#)

external [22](#)

internal [20](#)

mixed [23](#)

Derby [739](#)

diagnostics [172](#)

tools [172](#)

Distribution Directories [109](#)

Creating [118](#)

Deleting [122](#)

Editing [120](#)

Name [109](#)

Path [112](#)

Securing [114](#)

Distribution Directory Node [109](#)

DOCUMENT\_ROOT variable [725](#)

Domain [375](#)

domain templates, See resource templates

drill downs [336](#)

[336](#)

drivers [707](#), [708](#)

dssso.xml logon template file [689](#), [692](#)

Dynamic Language Switch [127](#)

## E

edasprof.prf [56](#)

effective policy [363](#)

Effective Policy dialog box [365](#)

Embedded BI Application [310](#)

Enable OLAP [553](#)

Enable(d) check box [136](#)

enabling the WebFOCUS servlet plug-in [541](#)

ENCRYPT command [663](#), [664](#), [684](#)

ENCRYPT parameter [684](#), [685](#)

encrypting procedures [686](#)

in Master Files [684](#)

encryption [18](#), [100](#), [481–483](#)

AES (Advanced Encryption Standard) [482](#),  
[483](#)

Default WebFOCUS encryption [482](#)

key [482](#), [483](#)

key file format [482](#)

ReportCaster [482](#)

security token [482](#), [483](#)

Enterprise resource template [378](#)

### events

- monitor log events [623](#)
- configuration events [603](#)
- content events [604](#)
- group events [606](#)
- Library access events [607](#)
- Magnify console events [608](#)
- ReportCaster configuration events [615](#)
- ReportCaster global update events [616](#)
- security events [603](#)

EVERYONE group [459](#)

EXIT command [711](#)

### exits

- WebFOCUS Server [709](#)

explicit groups [357](#)

external authentication [321](#)

external deployment [22](#)

External Security settings [147](#)

## F

FIELD option to RESTRICT attribute [665](#)

field values [670](#), [671](#)

- restricting access to [670](#), [671](#)

### fields

- restricting access to [668](#), [670](#)

Filter settings

- IBI\_URLFILTER [547](#)

filters [682](#)

Filters Settings [545](#)

- IBI\_CSRF\_Allow\_Legacy [545](#)

Filters Settings [545](#)

IBI\_CSRF\_Enforce [546](#)

IBI\_CSRF-Token\_Name [546](#)

IBI\_HTTP\_Response\_Header\_Cache\_Control  
[546](#)

IBI\_HTTP\_Response\_Header\_Enabled [546](#)

IBI\_HTTP\_Response\_Header\_Expires [546](#)

IBI\_MAX\_CONTENT\_SIZE [546](#)

IBI\_Rest\_Method\_Enforce [546](#)

IBI\_UPLOAD\_MAX\_MEMORY [547](#)

IBI\_XCONTENT\_TYPE\_OPTIONS [547](#)

IBI\_XSS\_Mode\_Block [547](#)

IBI\_XSS\_Protection [548](#)

folders [369](#)

changing title [375](#)

creating [372](#)

deleting [375](#)

duplicating [374](#)

publishing [373](#), [374](#)

viewing properties [369](#)

form variables [711](#)

## G

General Settings

IBIF\_excelservurl [536](#)

Get More Extensions [137](#)

Getting Started Workspace [377](#)

GETUSER [212](#)

Graph Settings

IBIF\_GraphAgents [537](#)

- group administrator [366](#)
- group events [606](#)
- Group Membership Report [453](#)
  - Creating [454](#)
- groups [357](#)
  - adding users [460](#)
  - administration [443](#)
  - administrator [366](#)
  - creating [366](#)
  - explicit and implicit [357](#)
  - Preconfigured [457](#)
  - privileges [18](#)
  - types of users [366](#)
  - understanding [455](#)
  - workspace groups [456](#)

## H

- HOLD files [657](#)
  - DBA security [657](#)
- HOLDSTAT files [657](#)
  - DBA security [657](#)
- Home Page
  - Redirect /ibi\_apps to [523](#)
- host headers [272](#)
- HTML5 Chart Extensions [135](#)
- HTML5 Chart Extensions Entries [136](#)
- HTTP BASIC Authentication [237](#)
- HTTP header variables [710](#), [725](#)
- HTTP request headers [175](#)
- HTTP\_ACCEPT variable [725](#)

- HTTP\_ACCEPT\_ENCODING variable [725](#)
- HTTP\_ACCEPT\_LANGUAGE variable [725](#)
- HTTP\_REFERER variable [725](#)
- HTTP\_USER\_AGENT variable [725](#)
- hybrid privileges [349](#)

## I

- IBFS [340](#)
- IBFS Path
  - Viewing [342](#)
- IBI\_Admin\_Name [150](#)
- IBI\_Admin\_Pass [150](#)
- IBI\_Allowed\_Cookies [551](#)
- IBI\_Anonymous\_User [150](#)
- IBI\_Anonymous\_WFRS\_Pass [150](#)
- IBI\_Anonymous\_WFRS\_User [150](#)
- IBI\_Approot\_Directory [522](#)
- IBI\_AUTO\_FEXOPTIONS [542](#)
- IBI\_AUTO\_SIGNOFF [526](#)
- IBI\_AUTO\_SIGNOFF\_MESSAGE\_DURATION [526](#)
- IBI\_AUTO\_TRACE [543](#)
- IBI\_AUTODESCRIBE [561](#)
- IBI\_Cache\_Effective\_Policies\_per\_Session\_Limit [565](#)
- IBI\_Cache\_Effective\_Policy\_Duration [565](#)
- IBI\_Cache\_User\_After\_Signoff\_Duration [566](#)
- IBI\_Cache\_Users\_Groups\_Duration [565](#)
- IBI\_Cache\_Users\_Groups\_Limit [566](#)
- IBI\_Cache\_WFC\_Fex\_Limit [566](#)
- IBI\_CASCADE\_SHARING [539](#)

- IBI\_CM\_Export\_WFRS\_File\_Extensions [535](#)
- IBI\_CM\_PRESERVE\_SOURCE\_INFO [535](#)
- IBI\_CM\_Zip [536](#)
- IBI\_CM\_Zip\_File\_Format [536](#)
- IBI\_CONCURRENT\_PUBLIC\_SESSION\_LIMIT [526](#)
- IBI\_CONCURRENT\_VISUALIZATION\_LIMIT [527](#)
- IBI\_CSRF\_Allow\_Legacy [545](#)
- IBI\_CSRF\_Enforce [546](#)
- IBI\_CSRF-Token\_Name [546](#)
- IBI\_Customized\_Signin\_Page [527](#)
- IBI\_DATAVALUES\_CACHE\_GLOBALPATHS [515](#)
- IBI\_DATAVALUES\_CACHE\_MAXMEG [518](#)
- IBI\_DEFAULT\_WELCOME\_PAGE [526](#)
- IBI\_DEFAULT\_WORKSPACE\_PATH [527](#)
- IBI\_Deferred\_Custom\_Description [542](#)
- IBI\_Deferred\_Notify\_Submitted [542](#)
- IBI\_Deferred\_Ticket\_Delete\_Confirm [542](#)
- IBI\_DESCRIBE\_TEMPLATES [561](#)
- IBI\_Email\_Server [551](#)
- IBI\_ENABLE\_CACHECOMS [551](#)
- IBI\_ENABLE\_INFOGRAPHICS [552](#)
- IBI\_ENABLE\_INLINED\_RESOURCE\_BUNDLES [529](#)
- IBI\_ENABLE\_LEGACY\_FEATURES [552](#)
- IBI\_Enable\_OLAP [553](#)
- IBI\_Enable\_Test\_Page [543](#)
- IBI\_Enable\_UDR [554](#)
- IBI\_Encryption\_Provider [544](#)
- IBI\_Exclude\_WFRS\_File\_Extensions [554](#)
- IBI\_Export\_Directory [522](#)
- IBI\_FOCALL\_DEFAULT [562](#)
- IBI\_Focus\_Warning\_Numbers [554](#)
- IBI\_Google\_Maps\_API\_Key [539](#)
- IBI\_Google\_Maps\_API\_Version [539](#)
- IBI\_Help\_Context [519](#)
- IBI\_Help\_Proxy\_Context [520](#)
- IBI\_Help\_Proxy\_Host [520](#)
- IBI\_HELP\_PROXY\_SECURE [520](#)
- IBI\_HOME\_PAGE\_CONFIGURATION [525](#)
- IBI\_HOME\_PAGE\_LEGACY\_LINKS [525](#)
- IBI\_HTTP\_Response\_Header\_Cache\_Control [546](#)
- IBI\_HTTP\_Response\_Header\_Enabled [546](#)
- IBI\_HTTP\_Response\_Header\_Expires [546](#)
- IBI\_Import\_Directory [522](#)
- IBI\_INDEX\_DESCRIPTION [554](#)
- IBI\_INFOSEARCH [555](#)
- IBI\_INFOSEARCH\_SOLR\_CLOUD [570](#)
- IBI\_INFOSEARCH\_SOLR\_TIMEOUT\_MILLISECONDS [570](#)
- IBI\_INFOSEARCH\_SOLR\_URL [570](#)
- IBI\_JS\_TRACE [543](#)
- IBI\_Lang [540](#)
- IBI\_Library\_Item\_Default\_Action [555](#)
- IBI\_Log\_Retain\_Days [522](#)
- IBI\_MAGNIFY\_RECORDLIMIT [571](#)
- IBI\_Mas\_Fullinfo [540](#)
- IBI\_MAX\_CONTENT\_SIZE [546](#)
- IBI\_Message\_Detail [530](#)
- IBI\_Mobile\_Favorites\_Proxy\_URL [530](#)
- IBI\_MOBILE\_VOICE [556](#)
- IBI\_Move\_Confirmation\_Message [530](#)

IBI\_Multiple\_Logins\_Per\_User [149](#)  
IBI\_OLAP\_Docked [551](#)  
IBI\_Olap\_SaveExcel [551](#)  
IBI\_Olap\_SaveExcel2000WithFormulas [551](#)  
IBI\_PROMPT\_FOR\_CONNECTION\_CREDENTIALS  
[556](#)  
IBI\_PUBLIC\_SESSION\_TIMEOUT [531](#)  
IBI\_Push\_Image [557](#)  
IBI\_Quick\_Data\_Form\_Only [565](#)  
IBI\_Quick\_Data\_Security [565](#)  
IBI\_REPORT\_CACHE\_ENABLE [518](#)  
IBI\_ReportCaster\_Context [521](#)  
IBI\_Repos\_DB\_Driver [566](#)  
IBI\_Repos\_DB\_Password [566](#)  
IBI\_Repos\_DB\_URL [566](#)  
IBI\_Repos\_DB\_User [566](#)  
IBI\_Repository\_Sync\_Interval [566](#)  
IBI\_REQUEST\_LOGGING [544](#)  
IBI\_RES\_GOV\_Advise [540](#)  
IBI\_ResourceBundle\_Alternate\_Prefixes [557](#)  
IBI\_Rest\_Method\_Enforce [546](#)  
IBI\_SCM\_Enable [567](#)  
IBI\_SCM\_Provider\_Type [567](#)  
IBI\_SCM\_Provider\_Version [567](#)  
IBI\_SCM\_PWA\_ENABLE [567](#)  
IBI\_SCM\_Repository\_Location [568](#)  
IBI\_SCM\_Root\_Project\_Location [568](#)  
IBI\_SCM\_Staging\_Directory [522](#)  
IBI\_SEARCH\_COLLECTION [571](#)  
IBI\_SEARCH\_PASSWORD [571](#)  
IBI\_SEARCH\_USERNAME [572](#)  
IBI\_Session\_Privilege\_Search\_Depth [531](#)  
IBI\_SESSION\_TIMEOUT [531](#)  
IBI\_Signin\_Message [531](#)  
IBI\_SIGNIN\_PATHS [557](#)  
IBI\_Site\_Profile [540](#)  
IBI\_Soap\_Detail [544](#)  
IBI\_TECHPREVIEW\_FEATURES [558](#)  
IBI\_Tempfiletimeout [541](#)  
IBI\_Temporary\_Directory [522](#)  
IBI\_TEXT\_GENERATION\_SERVER\_URL [573](#)  
IBI\_TOOL\_THEME [558](#)  
IBI\_Trace\_Directory [522](#)  
IBI\_Trace\_Retain\_Days [523](#)  
IBI\_Universal\_Profile [541](#)  
IBI\_Update\_Last\_Access [567](#)  
IBI\_UPLOAD\_MAX\_MEMORY [547](#)  
IBI\_URLFILTER [547](#)  
IBI\_User\_Namespace [151](#)  
IBI\_User\_Password\_Change [151](#)  
IBI\_V3\_DEFAULT\_LAYOUT [532](#)  
IBI\_V3\_PORTAL [532](#)  
IBI\_V4\_PORTAL [532](#)  
IBI\_Validate\_Action [574](#)  
IBI\_Validate\_Error\_Response [574](#)  
IBI\_Validate\_Response\_Header [574](#)  
IBI\_Webapp\_Context\_Default [521](#)  
IBI\_WEBAPP\_DEFAULT\_URL [521](#)  
IBI\_WebFOCUS\_Context [521](#)  
IBI\_WFDESCRIBE\_DEFAULT [562](#)

- IBI\_WFEXT [541](#)
- IBI\_WFTRANSINOUT [541](#)
- IBI\_XCONTENT\_TYPE\_OPTIONS [547](#)
- IBI\_XSS\_Mode\_Block [547](#)
- IBI\_XSS\_Protection [548](#)
- IBIF\_Active\_EXTJS [536](#)
- IBIF\_DbaPass\_Src [536](#)
- IBIF\_dbapass\_src variable [212](#)
- IBIF\_DESCRIBE\_NULL [560](#)
- IBIF\_excelservurl [536](#)
- IBIF\_GraphAgents [537](#)
- IBIF\_GraphservURL [537](#)
- IBIF\_Max\_Messages [538](#)
- IBIF\_odpEnable [550](#)
- IBIF\_olapPos [550](#)
- IBIF\_olapSkinColor [550](#)
- IBIF\_OlapSkinName [551](#)
- IBIF\_Persistentamp [537](#)
- IBIIMR\_PROMPTING [560](#)
- IBIMR\_domain variable [723](#)
- IBIMR\_PROMPTINGUNSET [561](#)
- IBIMR\_user variable [723](#)
- ibimultilanguage.js configuration file [513](#)
- IBIODP\_disable\_msg setting [550](#)
- IBIWF\_AS\_NAME\_REPORT [537](#)
- IBIWF\_Index [549](#)
- IBIWF\_Language [538](#)
- IBIWF\_mFrameName [549](#)
- IBIWF\_mOrder [549](#)
- IBIWF\_mPrefix [549](#)
- IBIWF\_mrColumns [549](#)
- IBIWF\_mReports [549](#)
- IBIWF\_mrRows [549](#)
- IBIWF\_Redirect [538](#)
- IBIWF\_RedirNewWindowSize [539](#)
- IF command [712](#), [721](#)
- IFDEF command [710](#), [712](#), [722](#)
- IFDEF command [710](#), [712](#), [722](#)
- implicit groups [357](#)
- INCLUDE command [710](#), [711](#), [715](#)
- inheritance [363](#)
- install.cfg configuration file [511](#)
- Integrated Windows Authentication [253](#)
- internal deployment [20](#)
- invoking WebFOCUS custom security plug-ins [715](#)
- invoking WebFOCUS servlet plug-ins [716](#)
- IP restriction filtering [29](#)
- J**
  - Java Container Security [238](#)
  - Java environment [176](#)
  - JEE Container Based Authentication [238](#)
  - JOIN command
    - data security [676–678](#), [681](#), [682](#)
  - JVM Property Information [176](#)
- K**
  - Kerberos [294](#), [295](#), [299](#)
    - constrained delegation [275](#)
    - Constrained Delegation [257](#)

Kerberos [294](#), [295](#), [299](#)

multi-domain environment [295](#)

unconstrained delegation [257](#)

key file format for encryption [482](#)

krb5.ini [295](#), [299](#)

## L

language selection on signin pages [127](#)

Legacy Home Page

Redirect /ibi\_apps to [524](#)

Library access events [607](#)

license code configuration [81](#)

local privileges [348](#)

logon templates for App Studio [689](#)

authentication template [692](#), [697](#)

cookie exception list [698](#)

how they work [689](#)

logon resource [692](#)

logon result [694](#)

optional logon parameters [695](#)

required logon parameters [694](#)

tags [692](#)

template file [697](#)

variables [695](#)

logon\_result tag [694](#)

## M

Magnify console events [608](#)

Magnify license [81](#)

Manage Private Resources [474](#)

Manage Rules on a Resource [365](#)

Managed Reporting [19](#), [560](#)

processing variables [723](#)

IBIMR\_domain variable [723](#)

IBIMR\_user variable [723](#)

internal variables [723](#)

MR\_FULL\_FEXNAME variable [723](#)

MR\_ITEM\_HANDLE variable [723](#)

plug-ins [716](#)

user IDs and passwords [723](#)

variables [723](#)

Managers Group [459](#)

Master Files [653](#), [664](#)

encrypting [684](#)

security attributes [653](#)

user access to [664](#)

MATCH command [663](#)

Microsoft Drill-Down Links [336](#)

mime.wfs configuration file [129](#), [512](#)

redirection settings [129](#)

mixed deployment option [23](#)

mode [184](#)

Monitor ID [627](#)

monitor log events [623](#)

MR\_FULL\_FEXNAME variable [723](#)

MR\_ITEM\_HANDLE variable [723](#)

Multiple Reports settings [549](#)

IBIWF\_Index [549](#)

IBIWF\_mFrameName [549](#)

IBIWF\_mOrder [549](#)

Multiple Reports settings [549](#)

    IBIWF\_mPrefix [549](#)

    IBIWF\_mrColumns [549](#)

    IBIWF\_mreports [549](#)

    IBIWF\_mrRows [549](#)

My Reports [369](#)

My Workspace [376](#)

My Workspace Group [457](#)

## N

Network Location [109](#)

New Start Page

    Redirect /ibi\_apps to [523](#)

NGXXJ server [100](#)

nlscfg.wfs configuration file [513](#)

nodes [97](#), [98](#), [100](#), [103–105](#)

    adding nodes to files [98](#), [104](#)

    changing a remote server node [100](#), [103](#),  
    [105](#)

NOPRINT option to RESTRICT attribute [665](#)

Null Behavior [560](#)

## O

obtaining the identity of the user [212](#)

odin.cfg configuration file [97](#), [512](#)

ODP\_target setting [550](#)

OLAP settings [550](#)

    IBI\_IBI\_Olap\_SaveExcel2000WithFormulas  
    [551](#)

    IBI\_OLAP\_Docked [551](#)

OLAP settings [550](#)

    IBI\_Olap\_SaveExcel [551](#)

    IBI\_Olap\_SaveExcel2000 [551](#)

    IBIF\_olapPos [550](#)

    IBIF\_olapSkinColor [550](#)

    IBIF\_OlapSkinName [551](#)

On Demand Paging settings

    \_search\_begin [550](#)

    IBIF\_odpEnable [550](#)

    IBIODP\_disable\_msg [550](#)

    ODP\_Target [550](#)

Open Portal Services [20](#)

OpenID Connect Authentication [239](#)

order of precedence [363](#)

Origins

    Cross-Origins Resource Sharing [160](#)

Other settings

    IBI\_Library\_Item\_Default\_Action [555](#)

    Enable OLAP [553](#)

    IBI\_Allowed\_Cookies [551](#)

    IBI\_Email\_Server [551](#)

    IBI\_ENABLE\_CACHECOMS [551](#)

    IBI\_ENABLE\_INFOGRAPHICS [552](#)

    IBI\_ENABLE\_LEGACY\_FEATURES [552](#)

    IBI\_Enable\_OLAP [553](#)

    IBI\_Enable\_UDR [554](#)

    IBI\_Exclude\_WFRS\_File\_Extensions [554](#)

    IBI\_Focus\_Warning\_Numbers [554](#)

    IBI\_INDEX\_DESCRIPTION [554](#)

    IBI\_Move\_Confirmation\_Message [530](#)



## Other settings

IBI\_PROMPT\_FOR\_CONNECTION\_CREDENTIALS  
556

IBI\_Push\_Image 557

IBI\_ResourceBundle\_Alternate\_Prefixes 557

IBI\_SIGNIN\_PATHS 557

IBI\_TECHPREVIEW\_FEATURES 558

IBI\_TOOL\_THEME 558

output variables 710, 711

Over Permitted 363

**P**

## Parameter Prompting settings

IBI\_AUTODESCRIBE 561

IBI\_DESCRIBE\_TEMPLATES 561

IBI\_FOCALL\_DEFAULT 562

IBI\_WFDESCRIBE\_DEFAULT 562

IBIF\_DESCRIBE\_NULL 560

IBIMR\_Prompting 560

IBIMR\_PROMPTINGUNSET 561

parameters 98, 104

password tag 694

passwords 653, 657–659

using the Remember Me feature 219

changing 657

DBA 658

for accessing data 212

PERMPASS 658, 659

setting externally 686

PATH\_INFO variable 725

PATH\_TRANSLATED variable 725

Paths to be executed on user Sign-in 557

Payment Card Industry (PCI) 727

Payment Card Industry Data Security Standard  
727

PCI Security Standards 727

PERMPASS SET parameter 658, 659

PERMPASS setting 212

plug-ins 707, 715

enabling 541

WebFOCUS Client 708

portals 19

Portals view 350

## Pre-Authentication

Central Authentication Service (CAS) 234

Custom Single Sign On (SSO) Authentication  
255

HTTP BASIC Authentication 237

Integrated Windows Authentication 253

JEE Container Based Authentication 238

OpenID Connect Authentication 239

Request Header Based Authentication 252

Trusted Ticket Authentication 310

Web Access Management Systems 250

precedence 363

privileges 347

categories 464

hybrid 349

local 348

Over Permitted 363

- privileges [347](#)
  - session [348](#)
  - types [347](#)
- procedures [686](#)
  - decrypting [686](#)
  - encrypting [686](#)
  - security [686](#)
- processing concepts
  - configuration files [709](#), [710](#)
  - drivers [707](#)
  - plug-ins [707](#)
  - script files [709](#), [710](#)
  - variables [710](#)
- profiles
  - specified servers in nodes [100](#), [103](#), [105](#)
- Properties panel [369](#)
- protecting
  - variables [481](#)
- proxy server configuration [22](#)
- Public access [227](#)
- public user [228](#)
  - BI Portal Availability [231](#)
- published resources [359](#)
- PVUIDXT (Pre-Verify User ID Exit) [709](#)

## Q

- QUERY\_STRING variable [726](#)
- Quick Data license [81](#)
- Quick Data settings
  - IBI\_Quick\_Data\_Security [565](#)

- Quick Data
  - IBI\_Quick\_Data\_Form\_Only [565](#)
  - settings [565](#)

## R

- read-only access [662](#), [670](#)
- read/write access [662](#)
- REBUILD command [663](#), [664](#)
  - user access to [664](#)
- Redirect /ibi\_apps to [523](#)
- Redirection Settings [129](#), [481](#)
- remote servers [98](#), [100](#), [103–105](#)
- REMOTE\_ADDR variable [726](#)
- REMOTE\_HOST variable [726](#)
- Report Library [20](#)
- ReportCaster [20](#)
- ReportCaster configuration events [615](#)
- ReportCaster global update events [616](#)
- ReportCaster Tab [75](#)
- Reporting Server [20](#)
- Repository Database Replication Utility [739](#)
- repository drivers [708](#)
- Repository settings
  - IBI\_Cache\_Effective\_Policies\_per\_Session\_Limit [565](#)
  - IBI\_Cache\_Effective\_Policy\_Duration [565](#)
  - IBI\_Cache\_User\_After\_Signoff\_Duration [566](#)
  - IBI\_Cache\_Users\_Groups\_Duration [565](#)
  - IBI\_Cache\_Users\_Groups\_Limit [566](#)
  - IBI\_Cache\_WFC\_Fex\_Limit [566](#)

## Repository settings

IBI\_Repos\_DB\_Driver [566](#)IBI\_Repos\_DB\_Password [566](#)IBI\_Repos\_DB\_URL [566](#)IBI\_Repos\_DB\_User [566](#)IBI\_Repository\_Sync\_Interval [566](#)IBI\_Update\_Last\_Access [567](#)

## Repository

Reconnection to Client [102](#)Request Header Based Authentication [252](#)REQUEST\_METHOD variable [726](#)resource templates [378](#)customizing [390](#)resources [350](#)publishing [359](#)sharing [359](#)Viewing on WebFOCUS Home Page [350](#)RESTRICT attribute [654](#), [663](#), [666](#), [668](#)keywords [663](#), [665](#)options [665](#)SAME option [665](#), [666](#)SEGMENT option [665](#), [666](#)VALUE option [665](#), [666](#)RESTRICT command [663](#)RESTRICT\_TO\_IP keyword [29](#)restricting access [668](#), [670](#)to data [653](#), [654](#), [663](#), [668](#)to fields [668](#), [670](#)to segments [668](#), [670](#)reverse proxy server configuration [22](#)roles [347](#)cloning [468](#)designing [367](#)managing [463](#)

rules

designing [368](#)managing [470](#)

Run Procedures With Different Connection

Credentials [559](#)Run With Different Connection Credentials [559](#)**S**SaaS Tenant resource template [378](#), [384](#)sMAAccountName [446](#)SAME option to RESTRICT attribute [665](#)script files [709](#), [710](#)SCRIPT\_NAME variable [726](#)Search Settings [570](#)IBI\_INFOSEARCH [555](#)IBI\_INFOSEARCH\_SOLR\_CLOUD [570](#)IBI\_INFOSEARCH\_SOLR\_URL [570](#)IBI\_MAGNIFY\_RECORDLIMIT [571](#)IBI\_MOBILE\_VOICE [556](#)IBI\_SEARCH\_COLLECTION [571](#)IBI\_SEARCH\_PASSWORD [571](#)IBI\_SEARCH\_USERNAME [572](#)security [653–655](#)App Studio logon templates [689](#)ACCESS [655](#), [668](#)access levels [662](#), [666](#), [668](#)

security [653–655](#)

DBA [653](#)

decrypting procedures [687](#)

defining requirements [339](#)

designing policy [17](#), [339](#)

encrypting data segments [684](#), [685](#)

encrypting Master Files [684](#)

encrypting procedures [686](#)

FOCUSID routine [686](#)

for FOCUS procedures [686](#)

identifying users [657](#), [658](#)

passwords [656](#), [661](#), [686](#)

planning [18](#)

RESTRICT [654](#)

storing DBA information centrally [676–678](#)

securitysettings-mobile.xml configuration file [512](#)

securitysettings-portlet.xml configuration file [512](#)

securitysettings-zone.xml configuration file [512](#)

SEGMENT option to RESTRICT attribute [665](#)

segments

encrypting [684](#), [685](#)

restricting access to [668](#), [670](#)

Self Service [562](#)

SelfService Developers Group [459](#)

SENDVAR command [712](#)

Server configuration

settings [88](#)

server nodes [97](#), [102](#), [103](#)

alternate [103](#)

clustered [97](#)

server nodes [97](#), [102](#), [103](#)

configuring [102](#)

Server security

edasprof.prf site profiles [106](#)

SERVER\_NAME variable [726](#)

SERVER\_PORT variable [726](#)

SERVER\_PROTOCOL variable [726](#)

SERVER\_SOFTWARE variable [726](#)

Server

adding [97](#)

configuration for Kerberos constrained

delegation [275](#)

configuring settings in Administration Console

[88](#)

security and variables [711](#), [712](#), [723](#)

settings [97](#)

session folder [200](#)

Session Monitor [183](#)

session privileges [348](#)

Session Timeout [123](#)

SET command [711](#), [723](#)

SET parameters [212](#), [657](#)

DBACSENSITIV [660](#)

DBAJJOIN [676](#)

PASS [657](#), [658](#), [661](#)

PERMPASS [212](#), [658](#), [659](#)

USER [657](#), [658](#), [661](#)

setting a permanent DBA password [658](#)

setting passwords externally [686](#)

sharing resources [359](#)

Side Menu [350](#)

signin pages language selection [127](#)

site profiles [106](#)

site.wfs configuration file [512](#)

Solr Settings

IBI\_INFOSEARCH\_SOLR\_TIMEOUT\_MILLISECONDS  
[570](#)

Source Code Management settings

IBI\_SCM\_Enable [567](#)

IBI\_SCM\_Provider\_Type [567](#)

IBI\_SCM\_Provider\_Version [567](#)

IBI\_SCM\_PWA\_ENABLE [567](#)

IBI\_SCM\_Repository\_Location [568](#)

IBI\_SCM\_Root\_Project\_Location [568](#)

sso\_logon\_resource tag [692](#)

Standard Reports [369](#)

subgroups [357](#)

subsystems [466](#)

## T

TABLE command [664](#)

template files [710](#)

templates for App Studio logon [689](#)

Text Generation Server Settings

IBI\_TEXT\_GENERATION\_SERVER\_URL [573](#)

TIBCO WebFOCUS [17](#)

TIBCO WebFOCUS Client [19](#)

TIBCO WebFOCUS components [19](#)

TIBCO WebFOCUS Reporting Server [20](#)

Tomcat [223](#)

trace files

how to save [200](#)

saving [199](#)

traces [172](#), [631](#)

All Clients [631](#)

Client Connector [631](#)

Web Services [634](#)

WFServlet [634](#)

Trusted connections [49](#)

trusted security

make a trusted connection [50](#)

Trusted Ticket Authentication [310](#)

Configuring [316](#)

## U

Unconstrained delegation

Kerberos [257](#)

universal profile [108](#)

update access [662](#)

Upload and Install Extensions Page [137](#)

upper command [721](#)

URL\_PROTOCOL variable [726](#)

USER attribute [657](#)–[659](#)

user identification [654](#)

user name tag [694](#)

users [445](#)

adding to groups [460](#)

advanced [366](#)

basic [366](#)

developer [366](#)

users [445](#)

    group administrator [366](#)

    Name Requirements [446](#)

## V

Validation settings

    IBI\_Validate\_Action [574](#)

    IBI\_Validate\_Error\_Response [574](#)

    IBI\_Validate\_Response\_Header [574](#)

VALUE option to RESTRICT attribute [665](#), [670](#),  
[671](#)

values [670](#)

    restricting user access to [670](#)

variable name tag [695](#)

variables [710](#), [723](#)

    for custom logon templates [695](#)

    for Managed Reporting processing [723](#)

    protecting [481](#)

verification tools [174](#)

verification

    Client connections and permissions [174](#)

View Rules on a Resource [365](#)

## W

Web Access Management System Authentication  
[250](#)

web browsers [19](#)

    configuring for Kerberos [279](#)

web server [19](#)

web server variables [725](#)

Web Services Settings

    trace [634](#)

WebFOCUS [17](#)

    Client [19](#)

    components [19](#)

    deployment options [17](#), [20](#)

    localizing [125](#)

    optional products [20](#)

    plug-ins [708](#)

    Security Center [444](#)

    security planning [18](#)

    Server [19](#)

webfocus.cfg configuration file [512](#)

WFEXT module [715](#)

WFS (WebFOCUS script) commands [710](#)

    CALL [711](#), [712](#)

    CONDITIONAL\_INCLUDE [711](#), [715](#)

    EXIT [711](#)

    IF [712](#)

    IFDEF [712](#)

    IFNDEF [712](#)

    INCLUDE [711](#), [715](#)

    SENDVAR [712](#)

    SET [711](#), [723](#)

    upper [721](#)

WFS (WebFOCUS script) files [710](#), [725](#)

WFS (WebFOCUS script) language syntax [713](#)

WFS (WebFOCUS script) logic INCLUDE [715](#)

WFServlet trace [634](#)

Workspace [375](#)

## Workspaces

[Getting Started 377](#)[My Workspace 376](#)[write-only access 662](#)

