



TIBCO® Product and Service Catalog

Security Guidelines

*Version 5.1.0
December 2022*



Contents

Contents	2
Introduction	4
HTTPS for Secure Connections to TIBCO Product and Service Catalog Application Server	5
Enabling SSL on JBoss WildFly Application Server	5
TIBCO Product and Service Catalog Cluster Environment Security	6
Secure Cache Server	7
Securing Connection among Nodes Using SSL	7
Secure Java Messaging Server	10
Configuring EMS over SSL	10
Security based on Authentication	11
Default Login Module	11
LDAP Login Module	12
Security based on Authorization or Roles	13
Role-based Security	13
Resource Security	14
Defining Resource Security	14
Selecting Resource Security Based on Resource Type	15
Adding and Selecting a Grantee	18
Secure Data Model Entities and Data	20
TIBCO Documentation and Support Services	21

Legal and Third-Party Notices	23
--	-----------

Introduction

This document describes guidelines to ensure security within the various components of TIBCO Product and Service Catalog.

HTTPS for Secure Connections to TIBCO Product and Service Catalog Application Server

Secure Sockets Layer (SSL) is a widely-used protocol for secure network communications. It encrypts network connections at the Transport Layer and is used in conjunction with HTTPS, the secure version of the HTTP protocol.

Set up the SSL to access the application through a browser over the HTTPS protocol for the JBoss WildFly application servers.

Enabling SSL on JBoss WildFly Application Server

Enable and verify SSL on JBoss WildFly Application Server.

By default, JBoss WildFly application server uses 8443 port for the HTTPS protocol. Type the following URL into your browser: `https://IPaddress:8443/eml/Login`.

By default, the application realm is mentioned in the `standalone.xml` file located in the `$JBOSS_HOME/standalone/configuration` directory. The `application.keystore` is auto generated on the first use with a self-signed certificate for *localhost*. However, generating the self-signed certificates are discouraged because they result in browser warnings on internal sites. Note:



Note: It is always good practice to create a custom application realm. For creating a custom application realm on JBoss WildFly application server, see [WildFly documentation](#).

TIBCO Product and Service Catalog Cluster Environment Security

TIBCO Product and Service Catalog clustered environment can be secured through web servers such as Microsoft IIS, Apache, or IBM HTTP web server. For instructions on how to set up other web servers, see the documentation provided by web server vendors.

Secure Cache Server

TIBCO Product and Service Catalog supports the Apache Ignite cache server. You can secure the cache server.

Securing Connection among Nodes Using SSL

By using the SSL socket communication, you can secure connection among all nodes of Apache Ignite.

Procedure

1. Navigate to `$MQ_HOME/config` and open the `IgniteMember.xml` file.
 - a. Set `sslContextFactory`: by default, Apache Ignite provides a default SSL context factory, `org.apache.ignite.ssl.SslContextFactory`, which uses a configured keystore to initialize SSL context.

```
<property name="sslContextFactory">
  <bean class="org.apache.ignite.ssl.SslContextFactory">
    <property name="keyStoreFilePath"
value="keystore/keystore.jks"/>
    <property name="keyStorePassword" value="123456"/>
    <property name="trustStoreFilePath"
value="keystore/truststore.ts"/>
    <property name="trustStorePassword" value="123456"/>
  </bean>
</property>
```

- b. Disable Certificate Validation: in some cases, you must disable certificate validation of the client side. For example, when connecting to a server with self-signed certificate

Set a disabled trust manager to `sslContextFactory`

```
<property name="sslContextFactory">
  <bean class="org.apache.ignite.ssl.SslContextFactory">
    <property name="keyStoreFilePath"
value="keystore/keystore.jks"/>
    <property name="keyStorePassword" value="123456"/>
    <property name="trustManagers">
      <bean class="org.apache.ignite.ssl.SslContextFactory"
factory-method="getDisabledTrustManager"/>
    </property>
  </bean>
</property>
```

- c. Set Protocol: By using Apache Ignite, you can configure different types of encryption. The following algorithms are supported <http://docs.oracle.com/javase/7/docs/technotes/guides/security/StandardName.s.html#SSLContext> and can be set by using the `setProtocol` method. The TLS encryption is the default.

```
<property name="sslContextFactory">
  <bean class="org.apache.ignite.ssl.SslContextFactory">
    <property name="setProtocol" value="SSL"/>
    ...
  </bean>
</property>
...
```

2. Save the `IgniteMember.xml` file.

Remember: If security is configured, the logs contain `communication encrypted=on`.

```
INFO: Security status [authentication=off, communication
encrypted=on]
```

The server console shows the following:

```
INFO: Security status [authentication=off, tls/ssl=on]
```

3. Generate `keyStore` using the following command:

```
keytool -genkey -alias ignite -keystore keystore.jks -keyalg RSA
```

4. Generate `trustStore` using the following two commands:

- ```
keytool -export -file ignite.cert -keystore keystore.jks -alias ignite
```
- ```
keytool -import -v -trustcacerts -file ignite.cert -keystore truststore.ts -alias ignite
```

For more information, see [Apache Ignite documentation](#).

Secure Java Messaging Server

TIBCO Product and Service Catalog uses the TIBCO Enterprise Messaging Service (EMS) Java messaging server. You need to configure TIBCO EMS for SSL.

Configuring EMS over SSL

You can configure the EMS server to start running over SSL.

Procedure

1. Stop the application server.
2. Edit the following values in `$EMS_HOME\tibco\cfgmgt\ems\data\tibemsd.conf` file.
 - specify the SSL protocol in the listen parameter: `listen=ssl://hostname:portno`
 - `ssl_server_identity = TIBCO_HOME/ems/version_number/samples/certs/server.cert.pem`
 - `ssl_server_key = TIBCO_HOME/ems/version_number/samples/certs/server.key.pem`
 - `ssl_password = manWjtSRCpaXu7hoTkDlcEPr6KNKRr`
 - `ssl_server_trusted =TIBCO_HOME/ems/version_number/samples/certs/client_root.cert.pem`

3. Start EMS server using the updated `tibemsd.conf` file.

```
TIBCO_HOME/ems/version_number/bin/tibemsd -config EMS_HOME/tibco/cfgmgt/ems/data/tibemsd.conf
```

The EMS server starts running over SSL.

Security based on Authentication

TIBCO Product and Service Catalog supports a variety of authentication methods and can be setup to work with many authentication servers including:

- LDAP
- Oracle Access Manager
- Computer Associates eTrust SiteMinder

By using a single password authentication, you can use the same password to access all systems. However, you still need to login to each system (for example, LDAP).

By using a single sign-on authentication, you can login once and have access to all applications including TIBCO Product and Service Catalog (for example, LDAP and SiteMinder).

Default Login Module

This is a basic login module, which is selected if no login module is configured. This login module is classified as "password-based authentication".

The default login module supports authentication for database as well as LDAP based users. For a user if Security Type=LDAP, the authentication goes to LDAP.

i Note: If explicit login module is set as LDAP, TIBCO Product and Service Catalog uses LDAP login module and not the Default login module.

- Users with security type = PASSWORD are managed in TIBCO Product and Service Catalog and authenticated within the application itself.
- Users with security type = LDAP must exist in configured LDAP server. Password is not captured as part of user profile.
- Users with security type = LDAP are validated against LDAP during user creation and update. No information is extracted from LDAP server - all the user profile is managed in TIBCO Product and Service Catalog. During creation, password is not

used while validating against LDAP. Only user existence is checked.

- User is validated against LDAP during user modify only if Security Type is changed from PASSWORD to LDAP.
- Password supplied during login is validated against LDAP during login.
- No automated user creation or update during login or single sign-on is supported.

LDAP Login Module

This is a login module for full LDAP integration. It is selected by configuring login module = LDAP in the Configurator. This login module can be classified as "password-based authentication" or "single sign-on" depending on configuration.

- Users with security type = PASSWORD are managed in TIBCO Product and Service Catalog and authenticated within the application itself. This works exactly like "Default login module".
- Users with security type = LDAP must exist in configured LDAP server. Password is not captured as part of user profile.
- Users with security type = LDAP are validated against LDAP during user creation and update. When user is created or modified explicitly using TIBCO Product and Service Catalog UI, Create User web service, or import metadata; information is not extracted from LDAP server. However, user must exist in LDAP. The profile information provided by the user is saved.

When login is attempted and if "auto update" is configured, some of the information provided during user creation is automatically updated with the information obtained from LDAP server.

Security based on Authorization or Roles

The TIBCO Product and Service Catalog server ensures that people can access only the data they are allowed to see. Authorization controls access to repository objects, pages, and menus based on users and roles.

Administrators must keep security in mind at all times when managing organizations, user, roles, and resources, because the security settings behind each of these rely on the others.

Role-based Security

Users' access privileges are defined by the roles assigned to the user by the TIBCO Product and Service Catalog Administrator. Privileges are based on the functions performed by a role.

Users might be assigned one or more roles, with each role granting the user a different access privilege and level. TIBCO Product and Service Catalog includes standard pre-defined, out-of-the-box user roles. You can define your own custom roles in addition to those to meet your specific business needs.

Role-based security in TIBCO Product and Service Catalog is determined by *negative logic*. TIBCO Product and Service Catalog checks which functions are *not* allowed. Role-based security works on functions associated with HTML elements. Functions identify a logical group of work, primarily menu items. For example, the repository function groups all repository related functions together.

There are two aspects of role-based security:

- **Dynamic menu generation:** If you change the user roles, the menus are updated the next time a page is refreshed.
- **Filtering HTML elements:** Certain HTML elements can be added or removed based on assigned user roles.

HTML elements are the hyper links such as the *add new record* link. You cannot control access to action links like 'modify', 'copy', and so on that appear against a list entry on a page. Security is applied after the page is built.

Resource Security

Resource security for users and roles can be set by an administrator. The application administrator can select one or more grantees. Moreover, the access control lists for grantees can be created for all or any specific resources. If a user and its role are selected as grantees, the user access permissions override the role permissions.

i Note: Names of the objects and permissions shown in these screens can be customized and may be different from what you see on your page.

Defining Resource Security

Use the Manage Resource Security page to select the specific resources for which you want to set the permissions.

Manage Resource Security

Resource Type

Repository ▼

Resources

ALL ▼

Show Permissions

Procedure

1. Select **Administration > Resource Security**. The Manage Resource Security page is displayed.
2. From the **Resource Type** drop-down list, select one of the following depending on what you want to set the permission for:
 - Event
 - Repository
 - Synchronization Profile
 - Work Item
 - Hierarchy

The **Resources** drop-down list is populated based on this selection.

3. From the **Resources** drop-down list, select the specific object for which you want to set the permission. If no event, repository, synchronization profile, work item, or hierarchy is present in the instance, the **Resources** drop-down list shows only the **ALL** option.
4. Click **Show Permissions**. Depending on the **Resource Type** selected, you can set permissions as listed in the following section. This also refreshes the page to show the grantee to whom the permission is assigned.

Selecting Resource Security Based on Resource Type

Before you begin

To view and set the permissions for a particular resource, you need to add grantee on the following pages:

- Manage Resource Security for Events
- Manage Resource Security for Repositories
- Manage Resource Security for Synchronization Profiles
- Manage Resource Security for Work Items
- Manage Resource Security for Hierarchies

Procedure

1. **Event:** When an event is selected as the **Resource Type** on the Manage Resource Security page, you can set permissions under **Resource Type** on the Manage Resource Security for Events page.
2. **Repository:** When a repository is selected as the **Resource Type** and a specific repository is selected in the **Resources** drop-down list of the Manage Resource Security page, you can set permissions for the following resources under **Resource Type** on the Manage Resource Security for Repositories page.
 - **Attribute Group:** You can set permissions for a specific attribute group within a repository. All available attribute groups for the selected repository are listed under the **Resources** drop-down list.

Attribute Group permissions are used when records are viewed, edited, or added. They are not applied when metadata is edited.
 - **Repository:** You can set permissions for the entire repository.

Following repository permissions apply to metadata management: Create, Modify, Input Mapping, Management of classifications, Rulebase management, View, Show usage, Copy, Delete, and Named version management.

The following repository permissions apply to record management: Import records, Browse Records, Export Records, Mass update records, and Text Search.
 - **Record:** You can set permissions for records within a single repository or all repositories in one go. The **ALL** option is available in the **Resources** drop-down list when a **Record** is selected. By default, the External User and Support Engineer roles are assigned for this permission.
 - **Relationship:** You can set permissions for a specific relationship of the repository. All available relationships for the selected repository are listed under the **Resources** drop-down list. Reverse relationships of the same repository are shown as separate entries. For example, if a repository has a cross-repository relationship, a contains (self forward), and a containedby (self reverse) relationships, all three are listed. However, the name of the reverse relationship for the cross-repository relationship is shown in the **Resources** drop-down list of the target repository.

For each relationship defined, permission can be allowed or denied for the following: Full control, Add new related record, Remove relationships, Modify

relationships attributes, Search records to add relationships, View relationships and related records.

Relationship permissions do not apply once the message is delivered to workflow. Relationships are used in workflow activities without resource security.

Relationships option is not displayed when there are no relationships defined for a repository.

- **Subset:** This option appears when you select **Resource Type** as **Repository** and **Resource** as a specific repository and the selected repository has Subset Rules created for it. This option allows you to set permissions based on a filter on repository records.
- **Classification Scheme:** You can set permissions for a specific classification scheme or all classification schemes within a repository. If the classification is not defined for a repository, the **Classification Scheme** option is not displayed in the **Resource Type** drop-down list.

If you select a single classification scheme from the **Resources** drop-down list, the following two permissions are displayed on which you can set the **Allow** or **Deny** permissions: Full Control and Browse Records by Classification.

If you select the **All** option from the **Resources** drop-down list, the Create Private Classification permission is displayed on which you can set the **Allow** or **Deny** permission.

By default, **Allow** is selected for Full Control. However, when the private classification scheme is created, the permission to browse private classification scheme is granted only to the user who created it and denied to all other roles.

For more information about Classification Scheme, see [Classification Schemes](#).

- **Perspective:** You can set permissions for a specific perspective within a repository. All available perspectives for the selected repository are listed under the **Resources** drop-down list.

For each perspectives defined, you can deny or allow permission for the following options: Full Control and Browse Records by perspective.

By default, **Allow** is selected for Full Control and Browse Records by perspective. However, if the user or role is denied permission to browse, they cannot see the name of the perspective on the drop-down menu on the record

UI.

If the perspective is not defined for a repository, the **perspective** option is not displayed in the **Resource Type** drop-down list.

3. **Synchronization Profile:** When a synchronization profile is selected as the **Resource Type** on the Manage Resource Security page, you can set permissions under **Resource Type** on the Manage Resource Security for Synchronization Profiles page.
4. **Work item:** When a work item is selected as the **Resource Type** on the Manage Resource Security page, you can set permissions under **Resource Type** on the Manage Resource Security for Work items page.
5. **Hierarchy:** On the Manage Resource Security page, if you select **Hierarchy** as the **Resource Type** and a specific hierarchy or all hierarchies from the **Resources** drop-down list, you can set permissions on the Manage Resource Security for Hierarchies page.

Adding and Selecting a Grantee

Procedure

1. Click **Add Grantee** in the **Manage Resource Security for <Resource Type>** page. The Select Grantee page is displayed.
2. Click **OK**.
3. Set the permissions as appropriate. You can allow or deny permissions for various actions. You can choose to deny or allow full control. Doing so overrides all other individually set permissions.

Each resource has default permissions. If you do not define any permission for the resource, the default value is used.

For example, the permissions that can be set for repositories are shown in the following figure.

Manage Resource Security for Repositories

Repository Name: ALL
 Repository Description: ALL
 Resource Type: Repository

[+ Add Grantee](#) [Delete Grantee](#)

Grantee	Type
<input checked="" type="radio"/> jsmith	User

Permission Name	Default	Allow	Deny
Full Control	Allowed	<input type="radio"/>	<input checked="" type="radio"/>
Browse Records	Allowed	<input type="radio"/>	<input type="radio"/>
Create	Allowed	<input type="radio"/>	<input type="radio"/>
Copy	Allowed	<input type="radio"/>	<input type="radio"/>
Delete	Allowed	<input type="radio"/>	<input type="radio"/>
Export Records	Denied	<input type="radio"/>	<input type="radio"/>

[Save](#) [Cancel](#)

4. Click **Save**.**Note:**

- The application allows the maximum possible permissions. If you "deny" all permissions and then specifically "allow" a permission for an object, "allow" overrides the "deny".
- Permissions defined for ALL resources of a type and permissions defined for specific resources of the type work independent of each other. The permission specified for a specific resource takes precedence on permissions specified on ALL. Permissions specified on ALL is default, it applies when same permission is not specified on a specific object. Setting permissions for "ALL" resources does not mean you cannot specify resource-specific permissions.

Secure Data Model Entities and Data

TIBCO Product and Service Catalog enables securing of data model entities such as repositories, attributes, attribute groups, relationships and relationship attributes by using the rulebase security based on certain conditions. In addition, it secures record data through the rulebase security. For information, see *TIBCO MDM Studio Rulebase Designer User's Guide*.

TIBCO Documentation and Support Services

For information about this product, you can read the documentation, contact TIBCO Support, and join TIBCO Community.

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the [TIBCO Product Documentation](#) website, mainly in HTML and PDF formats.

The [TIBCO Product Documentation](#) website is updated frequently and is more current than any other documentation included with the product.

Product-Specific Documentation

The following documentation for TIBCO® Product and Service Catalog is available on the [TIBCO® Product and Service Catalog Product Documentation](#) page.

- *TIBCO® Product and Service Catalog Release Notes*
- *TIBCO® Product and Service Catalog Installation and Configuration*
- *TIBCO® Product and Service Catalog Product Catalog Guide*
- *TIBCO® Product and Service Catalog User Guide*
- *TIBCO® Product and Service Catalog Web Services*
- *TIBCO® Product and Service Catalog Offer and Price Designer User Guide*
- *TIBCO® Product and Service Catalog Cloud Deployment*
- *TIBCO® Product and Service Catalog Security Guidelines*

How to Contact TIBCO Support

Get an overview of [TIBCO Support](#). You can contact TIBCO Support in the following ways:

- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the [TIBCO Support](#) website.

- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to [TIBCO Support](#) website. If you do not have a user name, you can request one by clicking **Register** on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the [TIBCO Ideas Portal](#). For a free registration, go to [TIBCO Community](#).

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 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 Cloud Software Group, Inc.

TIBCO, the TIBCO logo, and the TIBCO O logo are either registered trademarks or trademarks of Cloud Software Group, Inc. in the United States and/or other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: <https://scripts.sil.org/OFL>

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

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. CLOUD SOFTWARE GROUP, 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 Cloud Software Group, Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (<https://www.tibco.com/patents>) for details.

Copyright © 1999-2022. Cloud Software Group, Inc. All Rights Reserved.