TIBCO Runtime Agent™

Domain Utility User's Guide

Software Release 5.10
August 2015

Two-Second Advantage®

Important Information

Contents

Figures

Tables

Preface

This document gives comprehensive instructions on domain management tasks, such as creating domains, adding secondary servers, adding machines, configuring HTTPS and LDAP, and so on.

Topics

Changes from the previous Release of this Guide

All the screenshots have been updated with new TIBCO logo.

Related Documentation

This section lists documentation resources you may find useful.

TIBCO Runtime Agent Documentation

The TIBCO Runtime Agent™ software suite is a prerequisite for other TIBCO software products. In addition to Runtime Agent components, the software suite includes the third-party libraries used by other TIBCO products, TIBCO Designer™, Java Runtime Environment (JRE), TIBCO Rendezvous®, and TIBCO Hawk®.

The following documents form the TIBCO Runtime Agent™ documentation set:

- *TIBCO Runtime Agent™ Installation* Read this manual for instructions on site preparation and installation.
- *TIBCO Runtime Agent™ Installing Into a Cluster* Read this manual for instructions on installing TIBCO applications into a cluster environment.
- *TIBCO Runtime Agent™ Upgrading to Release 5.10.0* Read this manual for instructions on upgrading from release 5.x to release 5.10.0.
- *TIBCO Runtime Agent™ Domain Utility User's Guide* Read this manual for instructions on using TIBCO Domain Utility to create and manage administration domains.
- *TIBCO Runtime Agent™ Scripting Deployment User's Guide* Read this manual for instructions on using the AppManage scripting utility to deploy applications.
- *TIBCO Runtime Agent™ Authentication API User's Guide* Read this manual for instructions on using Authentication API.
- *TIBCO Runtime Agent™ Release Notes* Read the release notes for a list of new and changed features. This document also contains lists of known issues and closed issues for this release.

Other TIBCO Product Documentation

You may find it useful to read the documentation for the following TIBCO products:

- TIBCO Administrator™ : TIBCO Administrator allows you to manage users, machines and applications defined in a TIBCO administration domain. The TIBCO Administrator graphical user interface enables users to deploy, monitor, and start and stop TIBCO applications.

- TIBCO Designer™: This graphical user interface is used for designing and creating integration project configurations and building an Enterprise Archive (EAR) for the project. The EAR can then be used by TIBCO Administrator for deploying and running the application.
- TIBCO Hawk®: This is a tool for monitoring and managing distributed applications and operating systems.
- TIBCO Rendezvous®: Rendezvous enables programs running on many different kinds of computers on a network to communicate seamlessly. It includes two main components: the Rendezvous application programming interface (API) in several languages, and the Rendezvous daemon.
- TIBCO Enterprise Message Service™: This software lets application programs send and receive messages using the Java Message Service (JMS) protocol. It also integrates with TIBCO Rendezvous and TIBCO SmartSockets® messaging products.
- TIBCO ActiveMatrix BusinessWorks™: ActiveMatrix BusinessWorks is a scalable, extensible, and easy to use integration platform that allows you to develop integration projects. ActiveMatrix BusinessWorks includes a GUI for defining business processes and an engine that executes the process.
- TIBCO® Adapter software: TIBCO Runtime Agent is a prerequisite for TIBCO Adapter products. You will therefore find TIBCO Adapter product documentation useful.

Typographical Conventions

The following typographical conventions are used in this manual.

Table 1 General Typographical Conventions

Convention	Use
ENV_NAME *TIBCO_HOME* *TRA_HOME*	TIBCO products are installed into an installation environment. A product installed into an installation environment does not access components in other installation environments. Incompatible products and multiple instances of the same product must be installed into different installation environments. An installation environment consists of the following properties: • **Name** Identifies the installation environment. This name is referenced in documentation as *ENV_NAME*. On Microsoft Windows, the name is appended to the name of Windows services created by the installer and is a component of the path to the product shortcut in the Windows Start > All Programs menu. • **Path** The folder into which the product is installed. This folder is referenced in documentation as *TIBCO_HOME*. *TIBCO Runtume Agent* installs into a directory within a *TIBCO_HOME*. This directory is referenced in documentation as <ProductAcronym>*_HOME*. The default value of <ProductAcronym>*_HOME* depends on the operating system. For example on Windows systems, the default value is `C:\tibco\<ProductAcronym>\<ReleaseNumber>`.
`code font`	Code font identifies commands, code examples, filenames, pathnames, and output displayed in a command window. For example: Use `MyCommand` to start the foo process.
`bold code font`	Bold code font is used in the following ways: • In procedures, to indicate what a user types. For example: Type **`admin`**. • In large code samples, to indicate the parts of the sample that are of particular interest. • In command syntax, to indicate the default parameter for a command. For example, if no parameter is specified, `MyCommand` is enabled: `MyCommand [`**`enable`**` | disable]`

Table 1 General Typographical Conventions (Cont'd)

Convention	Use
italic font	Italic font is used in the following ways: • To indicate a document title. For example: See *TIBCO ActiveMatrix BusinessWorks Concepts*. • To introduce new terms For example: A portal page may contain several portlets. *Portlets* are mini-applications that run in a portal. • To indicate a variable in a command or code syntax that you must replace. For example: `MyCommand` *PathName*
Key combinations	Key name separated by a plus sign indicate keys pressed simultaneously. For example: Ctrl+C. Key names separated by a comma and space indicate keys pressed one after the other. For example: Esc, Ctrl+Q.
	The note icon indicates information that is of special interest or importance, for example, an additional action required only in certain circumstances.
	The tip icon indicates an idea that could be useful, for example, a way to apply the information provided in the current section to achieve a specific result.
	The warning icon indicates the potential for a damaging situation, for example, data loss or corruption if certain steps are taken or not taken.

Table 2 Syntax Typographical Conventions

Convention	Use
`[ ]`	An optional item in a command or code syntax. For example: `MyCommand [optional_parameter] required_parameter`
`|`	A logical `OR` that separates multiple items of which only one may be chosen. For example, you can select only one of the following parameters: `MyCommand param1 | param2 | param3`

Table 2 Syntax Typographical Conventions (Cont'd)

Convention	Use

`{ }`	A logical group of items in a command. Other syntax notations may appear within each logical group.
	
	For example, the following command requires two parameters, which can be either the pair `param1` and `param2`, or the pair `param3` and `param4`.
	
	`MyCommand {param1 param2} | {param3 param4}`
	
	In the next example, the command requires two parameters. The first parameter can be either `param1` or `param2` and the second can be either `param3` or `param4`:
	
	`MyCommand {param1 | param2} {param3 | param4}`
	
	In the next example, the command can accept either two or three parameters. The first parameter must be `param1`. You can optionally include `param2` as the second parameter. And the last parameter is either `param3` or `param4`.
	
	`MyCommand param1 [param2] {param3 | param4}`

Connecting with TIBCO Resources

How to Join TIBCOmmunity

TIBCOmmunity is an online destination for TIBCO customers, partners, and resident experts. It is a place to share and access the collective experience of the TIBCO community. TIBCOmmunity offers forums, blogs, and access to a variety of resources. To register, go to http://www.tibcommunity.com.

How to Access TIBCO Documentation

You can access TIBCO documentation here:

http://docs.tibco.com

How to Contact TIBCO Support

For comments or problems with this manual or the software it addresses, contact TIBCO Support as follows:

- For an overview of TIBCO Support, and information about getting started with TIBCO Support, visit this site:

  http://www.tibco.com/services/support

- If you already have a valid maintenance or support contract, visit this site:

  https://support.tibco.com

  Entry to this site requires a user name and password. If you do not have a user name, you can request one.

Chapter 1 Introduction

This chapter introduces TIBCO Domain Utility, which is used to manage administration domains.

Topics

Overview

TIBCO Domain Utility is installed as part of the TIBCO Runtime Agent™ installation. Domain Utility is used to create and manage administration domains. For an introduction to TIBCO Administrator and administration domains, see the *TIBCO Administrator User's Guide*.

Domain Utility is launched directly after installing TIBCO Administrator™ and is used to create the initial administration domain. Domain Utility can also be invoked later to perform the tasks described in Selecting a Task on page 8.

Domain Utility provides:

- Machine Management
  - — Add the machine on which Domain Utility is running to an existing administration domain.
  - — Join a logical machine to an administration domain. This task is used if you are configuring a domain to work within a cluster.
- Domain Configuration
  - — Create a new administration domain for an existing TIBCO Administrator installation.

The domain can use the default TIBCO Rendezvous transport for domain configuration, or be configured to use TIBCO Enterprise Message Service as the transport. Click the Show Advanced check box to change and configure the domain transport. See Creating a Domain that Uses a Database on page 53 for more information.

  - — Add a secondary server to an administration domain that uses TIBCO Rendezvous for domain communication.
  - — Delete an administration domain. The administration server and the TIBCO Hawk agent for the administration domain must be shutdown before proceeding with this task.
  - — Enable and configure HTTPS for a selected administration domain on the machine on which Domain Utility is running.

- Server Settings
  - Change the transport parameters used by TIBCO Administrator and TIBCO Hawk for a selected administration domain on the machine on which Domain Utility is running.
  - Change the domain administrator user name and password for a selected administration domain. The domain administrator user is the original user defined when creating the domain.
  - Change the Tomcat web server ports.
  - Change LDAP configuration for a selected administration domain.
  - Change database configuration for a selected administration domain.
- Migration
  - Upgrade 5.x domains to release 5.10.
- TIBCO EMS Plugin
  - Add a TIBCO Enterprise Message Service server to a selected administration domain.
  - Remove a TIBCO Enterprise Message Service server from a selected administration domain.
  - Update a TIBCO Enterprise Message Service server in a selected administration domain.
- Add a Servlet Engine Plugin
  - Add, update or remove a servlet engine plug-in.

GUI Mode or Command Line Mode

Domain Utility can be run in GUI mode, or in command line mode. Both modes are explained in this document.

Starting TIBCO Domain Utility in GUI Mode

You can start TIBCO Domain Utility in one of the following ways.

- Under Microsoft Windows:

  Choose **Start > All Programs > TIBCO > TIBCO Runtime Agent > Domain Utility**.

  or

  Invoke *TRA_HOME*`\bin\domainutility`

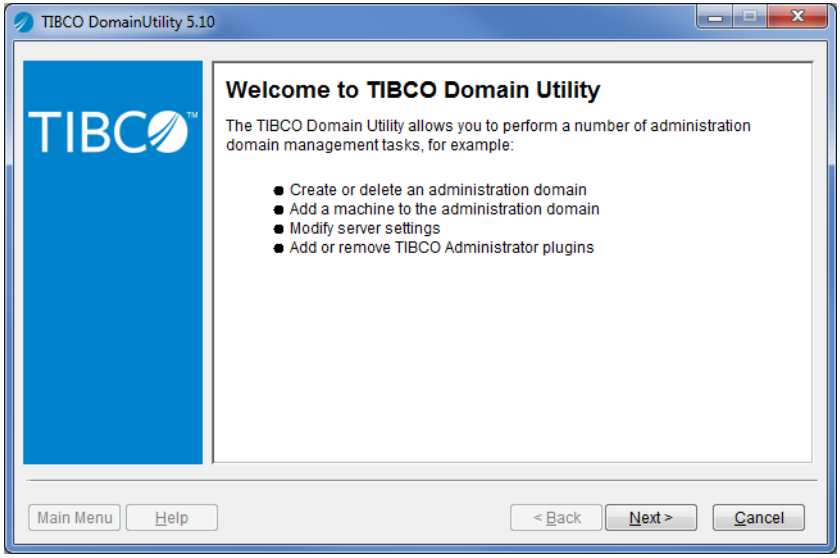
- Under UNIX:

  Invoke *TRA_HOME*`/bin/domainutility`

The next diagram shows the Domain Utility main page. Clicking the **Cancel** button closes Domain Utility. After you have selected a task, the **Main Menu** button becomes active.

If you click the **Main Menu** button, Domain Utility returns to the `Welcome` panel. If you have changed values in any fields, the values are lost.

Figure 1 Domain Utility Main Window



Domain Utility Log File

By default, the Domain Utility log file is written to the *TRA_HOME*`\logs\domainutility.log` file. You can change the log file location by adding the `java.property.logFile` *file-path-name* property to the *TRA_HOME*`\bin\domainutility.tra` file and providing a directory location.

Starting TIBCO Domain Utility in Command Line Mode

To run in command-line mode, use `domainutilitycmd`, which has the following syntax:

Prototype

TRA_HOME`\bin\domainutilitycmd`
`-cmdFile` *file*
`[-domain` *name*`]`
`[-usr` *user* `-pwd` *password*`]`
`[-logFile` *filename*`]`
`[-verbose]`
`[-lang` *locale*`]`
`[-help | -? | -h]`

While executing domain utility in command line mode on Linux, Unix, and AIX operating systems, you can get a info line on the command prompt. e.g. com.tibco.security.impl.np.SecurityVendor - Initializing Entrust crypto provider in NON FIPS 140-2 mode.

Parameters

Table 3 Parameters

-cmdFile	XML file that is used to execute a task. This XML file (not the command itself) defines the task. You can find template XML files in the following folder: *TRA_HOME*`\template\domainutility\cmdline` One task can be defined per file. The `domainutility.xsd` is included in the same folder. You can encrypt the passwords separately and use them in the cmdFile.
-domain	Administration domain to use for this task. The domain name is also specified in the XML file. If the domain is specified on the command line, it overrides the domain specified in the XML file.

Table 3 Parameters

-usr	User name to use for the task. The user name specified on the command line overrides the user name provided in the XML file.
-pwd	Password to use for the task. When specified, this value overrides the value provided in the XML file.
-logFile	Log file. If not provided, log information is written to *TRA_HOME*\logs\domainutility.log.
-verbose	If used, debug messages will be displayed on the console.
-lang	Language code for localization. See encoding in Domain Details on page 28 for details.
-help	Prints this usage.

Selecting a Task

The initial Domain Utility panel allows you to select a task to perform. After you have finished the task, you can restart Domain Utility to perform additional tasks. This section lists the tasks.

Machine Management

Table 4 Machine Management

Add Machine	Allows you to add the machine on which Domain Utility is running to an administration domain. The administration server for the domain must be running or you cannot add the machine to the domain. You can remove a machine from an administration domain using the TIBCO Administrator GUI. **Note**: If the administration domain is database-based, the machine you want to add must have direct access to the domain repository on the database server.
Manage Logical Machine	Allows you to add a node that is part of a cluster to an administration domain that is configured for a cluster environment.

Domain Configuration

This category displays only if you have TIBCO Administrator installed on your machine.

Table 5 Domain Configuration

Create a new Administration Domain	Use this task to create an administration domain. You can only perform this task if TIBCO Administrator has been installed.

Table 5 Domain Configuration

Add a secondary server	Allows you to add a secondary administration server to an existing administration domain if the primary administration server in the domain is already running. Secondary servers are used only in administration domains that use TIBCO Rendezvous as the transport. **Note:** You *cannot* promote a secondary server to a primary server.
Delete an Administration Domain	Use this task to delete an administration domain. The administration server and the TIBCO Hawk agent for the administration domain must be shutdown before proceeding with this task.
Enable HTTPS	Use this task to enable HTTPS for an administration domain which produces the following changes in behavior: • An HTTPS connection is required between the TIBCO Administrator GUI and the administration server. • HTTPS is added as an option for deployed applications to retrieve application data from the administration server. **Note:** This task does *not* enable secure communications between Hawk agents, which includes server actions like deploying, starting, and stopping applications. To secure communications between Hawk agents, use TIBCO Enterprise Message Service with SSL connections. Domain Utility supports self-signed certificates as well as certificates signed by a certificate authority. Click **Help** on each screen for additional information.

Server Settings

Table 6 Server Settings

Change Transport Parameters	Use this task to change the transport parameters used by the administration server and TIBCO Hawk Agent.
Update Domain Credentials	Use this task to change the username, password, or both for the administration user for a domain.

Table 6 Server Settings

Change Tomcat Web-Server Ports	Change the HTTP port, shutdown port, or shutdown string for the web server embedded in the Tomcat server.
LDAP Configuration	Change LDAP configuration for a selected administration domain.
Database Configuration	Change database configuration for a selected administration domain.
Miscellaneous	Update Max Deployment Revision value.

Migration

Table 7 Migration

Migration	Use this task to migrate a 5.x administration domain to release 5.10.0.

TIBCO EMS Plugin

Table 8 TIBCO EMS Plugin

Add TIBCO EMS Server	Creates a new mapping for a TIBCO Enterprise Message Service server so that it can be administered as part of an administration domain. **Note**: Domain Utility can verify the connection to the server only if Domain Utility is running on the machine on which the server is installed. As the product does not package EMS libraries, run traUpgradeManager with -ems option to set EMS client libraries in the tra file. See *TIBCO Runtime Agent 5.10.0 Installation Guide 5.10.0* for details.
Remove TIBCO EMS Server	Removes the mappings of a registered TIBCO Enterprise Message Service server from an administration domain.

Table 8 TIBCO EMS Plugin

Update TIBCO EMS Server	Changes the mappings of a TIBCO Enterprise Message Service server that is registered in an administration domain. **Note**: You cannot use this task to change the machine on which the server is deployed. Instead use the **Add TIBCO EMS Server** task.

Servlet Engine Plugin

Table 9 Servlet Engine Plugin

Add Servlet Engine	Add a servlet engine to a selected administration domain.
Remove Servlet Engine	Remove a servlet engine from a selected administration domain.
Update Servlet Engine	Update a servlet engine that is part of an administration domain.

Chapter 2

Machine Management and Domain Configuration

This chapter explains how to use Domain Utility to add machines to an administration domain and to create or modify domains.

Topics

Adding a Machine to a Domain

When you add a machine to an administration domain, the machine becomes visible in the TIBCO Administrator GUI `Machines` console in the `Resource Management` module. You can then use the `Application Management` console to deploy applications on the machine and start, stop, and monitor the applications using the TIBCO Administrator GUI.

The TIBCO Administrator GUI is used to remove a machine from an administration domain. See the *TIBCO Administrator User's Guide* for details.

- The machine you want to add to the domain must be able to access the domain repository on the database server directly if using a database back end.
- Domain Utility must be run from the machine that you want to add to the domain.
- The administration server for the domain must be running or you cannot add the machine to the domain.
- Only users with super user privileges in the administration domain can add machines to a domain. The domain administrator user name and password can also be used. These credentials were supplied when the domain was created.
- After adding a machine to a domain, you must start the TIBCO Hawk Agent that is created for the machine. Domain Utility will supply the executable name.
- If you are adding a virtual IP for a cluster group, you must select the Show Advanced check box to access the Domain Home Path Configuration and Cluster Group Configuration sections where you provide the location of the TIBCO Runtime Agent home directory on the cluster group's shared drive and the virtual IP address assigned to the cluster group.

To Add a Machine to a Domain Using the GUI

If a domain uses an SSL-enabled TIBCO Enterprise Message Service server for transport, you cannot add a machine to the domain using the TIBCO Domain Utility GUI. Use the command line utility instead and specify the applicable values in the `EMSParameters/SSL` element in `AddMachine.xml`. See To Add a Machine to a Domain Using the Command Line Utility on page 15.

1. On the machine to add, start Domain Utility and click the **Next** button on the main screen.
2. Under `Category`, select **Machine Management**, then select **Add Machine**. Click **Next**.
3. In the `Add Machine` panel, provide values in each field. See Add Machine Panel on page 16 for field descriptions.
4. Click **Next**. A summary dialog appears where you can verify that the values your provided are correct.
5. Click **Next** to add the machine to the domain.
6. Start the TIBCO Hawk Agent that is referenced in the last Domain Utility screen.

   On Microsoft Windows, a service is created using the domain name to which the machine has been added. Navigate to the Services panel and start the service.

   On Unix platforms, an executable is created in the *TIBCO_TRA_DOMAIN_HOME/domain-name* folder. Navigate to the folder and start the TIBCO Hawk Agent.
7. Click **Finish** to end the session.

To Add a Machine to a Domain Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\cmdline\AddMachine.xml`
3. Open `AddMachine.xml` in a text editor.

   Provide values for each parameter. See Add Machine Panel on page 16 for parameter descriptions.
4. After changing the parameters, save the file and exit the text editor.

5. Execute the following command to apply your changes to the domain:

   `domainutilitycmd -cmdFile` *working-dir-path*`\AddMachine.xml`

6. Start the TIBCO Hawk Agent that is associated with the machine.

   On Microsoft Windows, a service is created using the domain name to which the machine has been added. Navigate to the Services panel and start the service.

   On Unix platforms, an executable is created in the *TIBCO_TRA_DOMAIN_HOME/domain-name* folder. Navigate to the folder and start the TIBCO Hawk Agent.

Add Machine Panel

Table 10 Parameters for Adding Machine Panel

Username	Provide the name of a user who has super user privileges in the administration domain, or provide the domain administrator account name created when the domain was created.
Password	Password for the above user.
Domain	Click the Discover button to find an administration domain. If a domain does not appear, select **Show Advanced** and increase the **Discover Timeout** value. Check also that the transport used by the domain is selected.
Machine	This field lists the name of the machine that is being added to the domain. If you are adding a machine that is part of a cluster, you must change the given machine name to the virtual cluster hostname.
Hawk Cluster	Machines are grouped in the TIBCO Administrator GUI under the value provided in the `Hawk Cluster` field. If you change the default value, this machine displays in the TIBCO Administrator GUI under the value you provide. The cluster name must be enclosed within quotes, if the name contains spaces.
Advanced Options	

Table 10 Parameters for Adding Machine Panel

Show Advanced	Click to access advanced options.
Discover Timeout	Time Domain Utility allows for connecting to the master server. If no connection is made in the specified time, the master server may be down or slow to respond and Domain Utility times out. Increase this number on slow systems.
TIBCO Rendezvous TIBCO EMS	Select the transport to use for administration domain communication. The fields change, depending on the transport selection. The transport option you select will be used for all domain communication with the following exceptions: • For database-based domains, all clients and applications access the database server directly for domain data. • For domains integrated with LDAP, all clients and applications access the LDAP directory server directly for authentication. • You can customize applications to access application data locally or via HTTP, HTTPS, or the domain transport. **Note:** When adding a machine, you must select the transport already set for the primary domain. TIBCO Hawk and POF must use the same transport type. Mixed transport types are not supported. On selecting TIBCO EMS, you can edit the Hawk HMA parameters. Run traUpgradeManager with the -ems option to set EMS client libraries in the tra file, as the product no longer packages EMS libraries.
TIBCO Rendezvous parameters for TIBCO Administrator	
RV Daemon	TIBCO Rendezvous daemon used for client-server communication. Default is tcp:7500. For information about connecting to a remote daemon, see *TIBCO Rendezvous Concepts*. You must specify the same port used by the primary administration domain.

Table 10 Parameters for Adding Machine Panel

RV Network	TIBCO Rendezvous network used for client-server communication. This variable need only be set on computers with more than one network interface. If specified, the TIBCO Rendezvous daemon uses that network for all outbound messages.
RV Service	TIBCO Rendezvous service used for client-server communication. The Rendezvous daemon divides the network into logical partitions. Each transport communicates on a single service. A transport can communicate only on the same service with other transports. Unless you are using a non-default TIBCO Rendezvous configuration, you should use the default (7500).
TIBCO Rendezvous parameters for TIBCO Hawk	
Hawk Daemon	TIBCO Rendezvous daemon used for communication with TIBCO Hawk. Default is tcp:7474. See the *TIBCO Hawk Installation and Configuration* manual for details about this parameter.
Hawk Network	TIBCO Rendezvous network used for communication with TIBCO Hawk. Use the default unless you are an experienced TIBCO Rendezvous user. See the *TIBCO Hawk Installation and Configuration* manual for details about this parameter.
Hawk Service	TIBCO Rendezvous service used for communication with TIBCO Hawk. Use the default unless you are an experienced TIBCO Rendezvous user. Default is 7474. See the *TIBCO Hawk Installation and Configuration* manual for details about this parameter.
TIBCO EMS parameters for TIBCO Administrator	
Server URL	The URL of the TIBCO Enterprise Message Service server in the following format: `tcp://`*`hostname`*`:`*`port`*. If you have configured multiple fault tolerant servers, specify all of them here, separating them by commas. For example: `tcp://host1:7222,tcp://host2:7222`

Table 10 Parameters for Adding Machine Panel

Username	Specify the user account name authorized to administer the TIBCO Enterprise Message Service server. Specify a user that is a member of the `$admin` group (for example, the predefined `admin` user), or a user who has the following permissions:
	• publish, subscribe, and create permissions to the following topics:
	`com.tibco.pof.`*domain-name*`.>`
	`com.tibco.repo.server_discovery.>`
	`com.tibco.pof.AUTH_`*domain-name*`.>`
	`com.tibco.repo.instance_mgmt.*.trustworthy _HAWK.`*domain-name* `(for each domain)`
	• public, subscribe, and create permissions to the `com.tibco.repo.>` queues
	Note: You must add the following topics to the *TIBCO_HOME*`/ems/bin/topics.conf` file:
	`com.tibco.pof.`*domain-name*`.>`
	`com.tibco.repo.server_discovery.>`
	`com.tibco.pof.AUTH_`*domain-name*`.>`
	`com.tibco.repo.instance_mgmt.*.trustworthy _HAWK.`*domain-name* (one line for each domain)
	You must also add the following queue to the *TIBCO_HOME*`/ems/bin/queues.conf` file:
	`com.tibco.repo.>`
	Note that if *domain-name*, contains the characters '.', '>' and '*', the characters must be replaced by the following strings:
	"." replaced by "2E"
	">" replaced by "3E"
	"*" replaced by "%2A"

Password	Specify the password for the user account given in the Username field.
Enable SSL	Select to enable Secure Sockets Layer (SSL) for use with TIBCO Enterprise Message Service. See Enabling SSL for a TIBCO Enterprise Message Service Domain on page 22 for information about using SSL.
Domain Home Paths Configuration	

Table 10 Parameters for Adding Machine Panel

TRA Domain Home	Provide the location of the administration domain home that this machine is joining.
TIBCO Rendezvous parameters for TIBCO Hawk HMA	
Use default values	Select the **Use default values** check box unless you are an experienced user.
Hawk HMA Daemon	Hawk HMA Daemon instructs the transport creation function about how and where to find the Rendezvous daemon and establish communication. The default is tcp:7474
Hawk HMA Network	Hawk HMA Network specified, uses the specified network for all the communications.
Hawk HMA Service	Hawk HMA Service is used for client-server communication. Each transport communicates on a single service. A transport can communicate only on the same service with other transports. The default is 7475.
Cluster Group Configuration	
Machine is Logical	Select if the administration domain is installed in a cluster group. If you have provided an IP address in the Machine field, the IP address displays in the Virtual IP Address field after this field is selected.
Virtual IP Address	You can add a value to this field, or change the value in this field to another IP address. The address must be that of the virtual cluster group. If you change the IP address, the value in this field will be validated, not the value in the Machine field.
Property Files Group Name	

Authorized Group Name	This property is used to secure the `.properties` files. The specified group will be given view access to the `AuthorizationDomain.properties` and `AdministrationDomain.properties` files when these property files are created as part of domain creation. Specifying this property allows the users in the specified group to use TRA utilities like `AppManage`.

Enabling SSL for a TIBCO Enterprise Message Service Domain

SSL is a protocol for transmitting encrypted data over the Internet or an internal network. SSL works by using public and private keys to encrypt data that is transferred over the SSL connection. See the *TIBCO Enterprise Message Service User's Guide* for general information about the SSL protocol and specific information about file types for digital certificates.

The following parameters are set when configuring SSL for a domain that uses an Enterprise Message Service server.

Table 11 Parameter Set for Configuring SSL

Do Not Verify Host	Specifies whether the client should verify the server's certificate. When cleared, the client should verify the server's certificate. This is recommended. When selected, the client establishes secure communication with the server, but does not verify the server's identity.
Trusted	List of CA certificates to trust as issuers of server certificates. Supply only CA root certificates.
Identity	The client's digital certificate. Supply a certificate in either PEM or PKCS#12 format. You must also supply a private key file in the Private Key field if you supply a PEM-formatted certificate here.
Private Key	The name and location of the client's private key file. This key must be in PKCS#8 format.
Password	Password for client's private key.

Table 11 Parameter Set for Configuring SSL

Do Not Verify Hostname	Specifies whether the client should verify the name in the CN field of the server's certificate. When cleared, the client should verify the name of the connected host or the name specified in the Expected Hostname field against the value in the server's certificate. If the names do not match, the connection is rejected. When selected, the client establishes secure communication with the server, but does not verify the server's name.
Expected Hostname	The name the client expects in the CN field of the server's certificate. If this parameter is not set, the expected name is the hostname of the server. The value of this parameter is used when the Do Not Verify Hostname parameter is cleared.
Cipher Suite Names	Specifies the cipher suites that the client can use. Supply a list of cipher names by clicking Add and selecting from the pull down menu that appears. Remove an entry from the list by selecting the entry and clicking Remove. Make an in place change to the list by selecting an entry and clicking Edit. Select a replacement entry from the pull down menu that appears. For more information, see Specifying Cipher Suites in the *TIBCO Enterprise Message Service User's Guide*.

Joining a Logical Machine to a Domain

Use this command to add a node that is part of a cluster group to an administration domain. Each node in a cluster group must have access to the domain files on a shared drive, so that fail-over can proceed seamlessly. For this, information about the TIBCO Runtime Agent domain home paths must be propagated to all nodes in a cluster group. (Note that a node may be referred to as a logical machine. All nodes in a cluster group have the same virtual-machine name, a virtual IP address, or a cluster group name.)

After you join a logical machine to a domain, TIBCO Domain Utility updates the TIBCO Runtime Agent domain home and TIBCO Administrator domain home information in the `DomainHomes.properties` file. On Microsoft Windows platforms, Domain Utility also registers the TIBCO Hawk and TIBCO Administrator services.

See the *TIBCO Runtime Agent Installing Into a Cluster* guide for more information.

To Add a Logical Machine to a Domain Using the GUI

1. On the machine to add, start Domain Utility and click the **Next** button on the main screen.
2. Under `Category`, select **Machine Management**, then select **Manage Logical Machine**. Click **Next**.
3. In the `Join Logical Machine to Domain` panel, click **Add** and in the dialog that displays, provide values in each field. See Join Logical Machine Panel on page 25 for field descriptions.
4. Click **Next**. A summary dialog appears where you can verify that the values your provided are correct.
5. Click **Next** to add the logical machine to the domain.
6. Click **Finish** to end the session.

To Add a Logical Machine to a Domain Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\cmdline\JoinLogicalMachine.xml`
3. Open `JoinLogicalMachine.xml` in a text editor.

Provide values for each `JoinLogicalMachine` element. See Join Logical Machine Panel on page 25 for element descriptions.

4. After changing the element values, save the file and exit the text editor.
5. Execute the following command to apply your changes to the domain:

   ```
   domainutilitycmd -cmdFile
   working-dir-path\JoinLogicalMachine.xml
   ```

Join Logical Machine Panel

Table 12 Join Logical Machine Panel

Domain	Provide the name of the administration domain to join.
Logical Machine	Provide the cluster group's network name or virtual IP address.
TRA Domain Home	Click the**...** button to select the location of the TIBCO Runtime Agent domain home folder on the cluster group's shared drive. The default location is `C:\tibco\tra\domain`.
Administration Domain Home	If this node is to serve as a backup to the administration server, click the**...** button to navigate to the location of the administration domain home on the cluster group's shared drive. For example, `C:/tibco/administrator/domain`. If the node is not to be used as a backup, do not enter information in the field.

Creating a Domain that Uses a File Repository

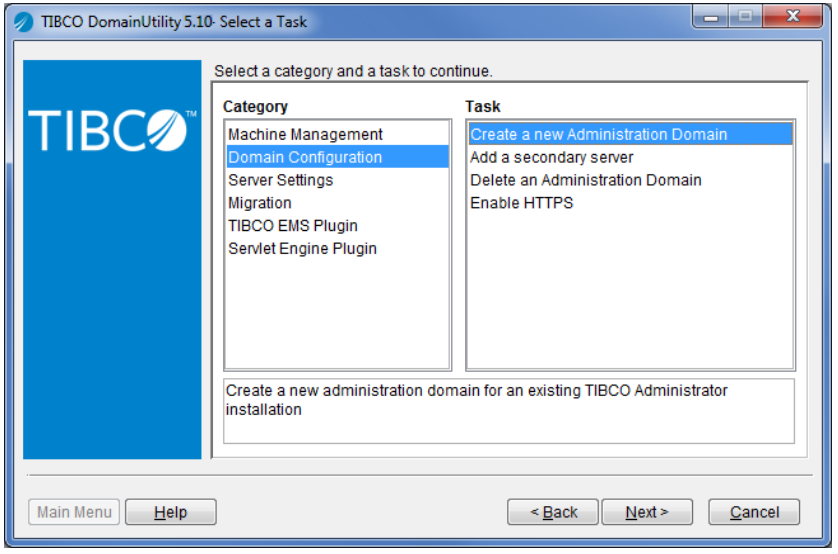
Use this procedure to create an administration domain that uses a file based domain repository to store users, groups and other domain information. You can only perform this procedure if TIBCO Administrator has been installed. If TIBCO Administrator is not installed, the Domain Configuration category will not display in TIBCO Domain Utility. A machine can have multiple administration domains installed.

You can only create an administration domain that uses a file repository if the domain transport is TIBCO Rendezvous. If TIBCO Enterprise Message Service is configured as the transport, the domain must use a database repository for storage.

To Create a File Based Repository Domain Using the GUI

1. Start Domain Utility and click the **Next** button on the main screen.
2. Under `Category`, select **Domain Configuration** and select **Create a New Administration Domain**. Click the **Next** button. A screen similar to the following appears.

Figure 2 Select a Task Window



3. Provide domain details. See Domain Details on page 28 for field descriptions.

4. Do not select the `User and Group information retrieved from a corporate LDAP` and `Domain information stored in a Database` options.

   If you need to change the TIBCO Rendezvous parameters used to communicate with TIBCO Administrator or TIBCO Hawk, select **Show Advanced**. See Domain Details on page 28 for a description of each parameter.

5. Click the **Next** button. The screen that appears allows you to change the default ports TIBCO Administrator uses to communicate with the Tomcat web server. In most cases, the default settings are appropriate. See Web Server Ports on page 35 for a description of the ports.

6. Click the **Next** button to continue. In the screen that appears, provide the domain administrator credentials for the administration domain. The user name and password given here is used when launching TIBCO Administrator to initially log into the administration domain and assign permissions to other users, so they can access certain components. The administration credentials are also used if you need to modify this domain.

   By default, a password policy is not defined. To use a password policy, select the Configure Password Policy check box. The fields that display are explained on Password Policy on page 36.

7. Click the **Next** button. The screen that appears displays a summary of the values you have provided.

8. Click the **Next** button to create the administration domain. After the domain has been created, the services that support the domain are listed. You must start each service before starting TIBCO Administrator.

9. Click **Finish** to end the session.

After creating the domain, `hawkhma.cfg` and tibhawkhma.tra files are generated.

To Create a File Based Repository Domain Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.

2. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\cmdline\CreateDomain.xml`

3. Open `CreateDomain.xml` in a text editor.

   The `CreateDomain.xml` file contains sections for creating a domain that uses a repository, LDAP server and database. Change only the repository section. The parameters for a domain that uses a repository are explained in the

following sections. After changing the parameters, save the file and exit the text editor.

4. Execute the following command to apply your changes to the domain:

```
domainutilitycmd -cmdFile <working-dir-path>\CreateDomain.xml
```

Domain Details

Table 13 Parameters for Creating a Domain

Domain Details	
Administration Domain	Name of the administration domain, which will also be the name of the server itself. Choose a name that clearly identifies the administration domain. Do not choose the name of the network domain. If an administration server (with or without security) is already running in the subnet, you cannot use that name for a second server with the same TIBCO Rendezvous parameters. If an administration server (with or without security) is already running in the same machine, you must use a different name for a second server. Domain name length must be less than 60 characters. You can use alphanumeric characters, hyphen (-), or under bar (_). Other characters, including period or comma, are not allowed.
Project Directory	Provide the location where the server looks for the domain data store, for project files saved as single-file projects, and for deployment configuration files. A default location is given.
Machine	The name of the machine on which the domain is installed.
Hawk Cluster	Machines are grouped in the Administrator GUI under the value provided in the `Hawk Cluster` field. If you change the default value, this machine displays in the Administrator GUI under the value you provide. The cluster name must be enclosed within quotes, if the name contains spaces.

Table 13 Parameters for Creating a Domain

Encoding	The encoding option is used for communication between the administration server and its clients. Choices are ISO8851 and UTF-8. This encoding is used for all primary and secondary servers in the administration domain. The default is ISO8859-1 (Latin-1) encoding by default. The value is used for the following properties in the `tibcoadmin<`*domain*`>.tra` file: • tibcoadmin.client.encoding Encoding used to encode the HTML sent to the web browser • file.encoding Property file (.tra file) encoding format • repo.encoding Encoding used by TIBCO Administrator and other products to communicate In some situations, it may be necessary to choose UTF-8 as the encoding for all or some of these properties. For example, If you are using XML messages and either the JMS transport or the AE/RV wireformat, you must change `repo.encoding` to UTF-8. If you are using a property file (.tra) that uses non-Latin1 characters, you must change file.encoding to UTF-8. You can edit the individual properties in the `.tra` file, or set the encoding for all three properties here.
Domain Data Store Configuration	
User and Group information retrieved from a corporate LDAP	Select if you are using a corporate LDAP server to manage users and groups. You will be prompted later to provide connection parameters to the LDAP server and search parameters for users and groups.
Domain information stored in a Database	Select if you are storing user and group information in a database. You will be prompted later for connection information to the database. It is checked by default.

Table 13 Parameters for Creating a Domain

Local Application Data	When selected, the repository instance and other deployment files is written to each target machine to which the service instance is deployed. This allows the instance to run independently of the administration server. When cleared, a repository instance for the service instance is created on the administration server and the remote repository instance is referenced in each service instance's property file (.tra file). This requires the service instance to query the administration server at runtime. It's checked by default.
Advanced Options	
Show Advanced	Select to specify the transport that administration domain components will use for communication. For an existing domain, select to change the default parameters of the domain transport or TIBCO Hawk, or to set the domain home paths and configure a cluster group if the domain is to be used inside a cluster. The transport option you select will be used for all domain communication with the following exceptions: • For database-based domains, all clients and applications access the database server directly for domain data. • For domains integrated with LDAP, all clients and applications access the LDAP directory server directly for authentication. • You can customize applications to access application data locally or via HTTP, HTTPS, or the domain transport. **Note:** TIBCO Hawk and POF must use the same transport type. Mixed transport types are not supported.
TIBCO Rendezvous parameters for TIBCO Administrator	
RV Daemon	TIBCO Rendezvous Daemon used for client-server communication. Default is tcp:7500.

Table 13 Parameters for Creating a Domain

RV Network	TIBCO Rendezvous network used for client-server communication. This variable need only be set on computers with more than one network interface. If specified, the TIBCO Rendezvous daemon uses that network for all outbound messages.
RV Service	TIBCO Rendezvous service used for client-server communication. The Rendezvous daemon divides the network into logical partitions. Each transport communicates on a single service. A transport can communicate only on the same service with other transports. Unless you are using a non-default TIBCO Rendezvous configuration, you should use the default (7500).
TIBCO Rendezvous parameters for TIBCO Hawk	
Hawk Daemon	TIBCO Rendezvous Daemon used for communication with TIBCO Hawk. Default is tcp:7474. See the *TIBCO Hawk Installation and Configuration* manual for details about this parameter.
Hawk Network	TIBCO Rendezvous network used for communication with TIBCO Hawk. Use the default unless you are an experienced TIBCO Rendezvous user. See the *TIBCO Hawk Installation and Configuration* manual for details about this parameter.
Hawk Service	TIBCO Rendezvous service used for communication with TIBCO Hawk. Use the default unless you are an experienced TIBCO Rendezvous user. Default is 7474. See the *TIBCO Hawk Installation and Configuration* manual for details about this parameter.
TIBCO EMS parameters for TIBCO Administrator	
Server URL	The URL of the TIBCO Enterprise Message Service server in the following format: `tcp://`*`hostname`*`:`*`port`*. If you have configured multiple fault tolerant servers, specify all of them here, separating them by commas. For example: `tcp://host1:7222,tcp://host2:7222`

Table 13 Parameters for Creating a Domain

Username	Specify the user account name authorized to administer the TIBCO Enterprise Message Service server. Specify a user that is a member of the `$admin` group (for example, the predefined `admin` user), or a user who has the following permissions:
	• publish, subscribe, and create permissions to the following topics:
	`com.tibco.repo.>`
	`com.tibco.pof>`
	`or`
	`com.tibco.pof.HawkConfig.>`
	`com.tibco.pof.MonitoringManagement.>`
	`com.tibco.repo.server_discovery.>`
	`com.tibco.pof.`*`domain-name`*`.> (for each domain)>`
	`com.tibco.pof.AUTH_`*`domain-name`*`.> (for each domain)`
	`com.tibco.repo.instance_mgmt.*.trustworthy_HAWK.`*`domain-name`* `(for each domain)`
	• publish, subscribe, and create permissions to the `com.tibco.repo.>` queues
	Note: You must add the following topics to the *TIBCO_HOME*`/ems/bin/topics.conf` file:
	`com.tibco.pof.`*`domain-name`*`.>`
	`com.tibco.repo.server_discovery.>`
	`com.tibco.pof.AUTH_`*`domain-name`*`.>`
	`com.tibco.repo.instance_mgmt.*.trustworthy_HAWK.`*`domain-name`* (one line for each domain)
	You must also add the following queue to the *TIBCO_HOME*`/ems/bin/queues.conf` file:
	`com.tibco.repo.>`
	Note that if *domain-name*, contains the characters '.', '>' and '*', the characters must be replaced by the following strings:
	"." replaced by "2E"
	">" replaced by "3E"
	"*" replaced by "%2A"

Password	Specify the password for the user account given in the Username field.

Table 13 Parameters for Creating a Domain

Enable SSL	Select to enable Secure Sockets Layer (SSL) for use with TIBCO Enterprise Message Service. See Enabling SSL for a TIBCO Enterprise Message Service Domain on page 22 for information about using SSL.
Domain Home Paths Configuration	
TRA Domain Home	Click the**...** button and navigate to a drive shared by all nodes in the cluster. Specify the location of the TIBCO Runtime Agent domain home. For example, `R:\tibco\tra\domain`. See the *TIBCO Runtime Agent Installing in a Cluster* guide for more information.
Administration Domain Home	Click the**...** button and navigate to a drive shared by all nodes in the cluster. Specify the location of the administration server domain home. For example, `C:\tibco\administrator\domain`.
TIBCO Rendezvous parameters for TIBCO Hawk HMA	
Use default values	Select the **Use default values** check box unless you are an experienced user.
Hawk HMA Daemon	Hawk HMA Daemon instructs the transport creation function about how and where to find the Rendezvous daemon and establish communication. The default is tcp:7474.
Hawk HMA Network	Hawk HMA Network specified, uses the specified network for all the communications.
Hawk HMA Service	Hawk HMA Service is used for client-server communication. Each transport communicates on a single service. A transport can communicate only on the same service with other transports. The default is 7475.
Cluster Group Configuration	
Machine is Logical	Select if the value entered in the Machine field is a logical machine. See the *TIBCO Runtime Agent Installing in a Cluster* guide for more information.

Table 13 Parameters for Creating a Domain

Virtual IP Address	Optional. Provide the cluster virtual IP address.
Symmetric Key	
Symmetric Key	Select to use dynamically generated keys to encrypt sensitive data by default when deploying applications locally. A static key is used if this checkbox is cleared. **Note:** This option does *not* affect sensitive data in the deployment configuration files exported using the `AppManage` utility. See *TIBCO Runtime Agent Scripting Deployment Guide* for information on how to protect sensitive data in the deployment of configuration files using an encryption password.
Max Deployment Revision	
Max Deployment Revision	Specify the default number of application revisions to keep in the revision history for each deployed application. Leave the value at `-1` to keep all revisions by default.

Table 13 Parameters for Creating a Domain

Property Files Group Name	
Authorized Group Name	This property is used to secure the `.properties` files. The specified group will be given view access to the `AuthorizationDomain.properties` and `AdministrationDomain.properties` files when these property files are created as part of domain creation. Specifying this property allows you in the specified group to use TRA utilities like `AppManage`.

Multiple Administration Domains on One Machine

If you decide you wish to use multiple administration domains on one machine, the domain names have to be different. Note that you cannot use the same TIBCO Rendezvous Service and two different TIBCO Rendezvous daemons parameters. For example, you *cannot* choose:

Table 14 Parameters for Multiple Domain

	Domain1	Domain2
Daemon	tcp:7500	tcp:7999
Service	7500	7500 (will not come up)

All other combinations of service and daemon are allowed.

Web Server Ports

The ports TIBCO Administrator uses to communicate with the Tomcat web server are described next. A *Connector* represents an endpoint by which requests are received and responses are returned. A connector is associated with a port.

Table 15 Web Server Ports

HTTP Port	A non-SSL HTTP 1.1 Connector. Defaults to 8080 for the first server installed and is incremented by 10 for additional servers (e.g. 8090 for the second server).
Shutdown Port	The web server listens for shutdown commands on this port.

Table 15 Web Server Ports

Shutdown String	A string for the shutdown command. Change it to from SHUTDOWN for security. **Note:** This shutdown string is not considered a password and is not checked against the password policy.

Password Policy

You can specify a password policy for the domain. See the *TIBCO Administrator Server Configuration Guide* for an introduction to the administration domain password policy. You can change the password policy after the administration domain has been created. See the *TIBCO Administrator User's Guide* for details.

The password policy applies to all users and groups in the administration domain. You should use an LDAP directory server if you want to customize password policies for different users and groups.

Table 16 Password Policy

Username	Provide the name of the domain administrator who will initially log into TIBCO Administrator and authorize other users to do so.
Password	Provide a password for that user. The password you provide is dependent on the password policy you choose. The policy choices are described below.
Confirm Password	Renter the password.
No Policy	If selected, no policy is enforced for passwords created in the domain. This allows user accounts to be created in the domain using the TIBCO Administrator GUI without assigning passwords.

Table 16 Password Policy

Default Policy	If selected, the following password policy is enforced. A password: • Is saved in encryption mode using a fixed key (Refer to *TIBCO Runtime Agent Installation* for more information about Obfuscate Utility). That is, SaveHashMode is set to false. • Must contain at least three characters.
Restrictive Policy	If selected, the following password policy is enforced. A password: • Is saved in hash mode using SHA1 algorithm. That is, SaveHashMode must be set to true. • Must contain at least eight characters. • Cannot contain the current password. • Cannot contain the user's name. • Cannot contain the space character. • Must contain at least three of the following: — One or more characters in lower case (a-z) — One or more characters in upper case (A-Z) — One or more numeric characters (0-9) — One or more punctuation characters (,!@#$%^&*()_+ | ~-=\`{}[]:";'<>?,./) • A password must be changed after 90 days. • A password must be changed on a user's first login or when the password is reset. • A user account is disabled after five failed login attempts. • The last five passwords used cannot be reused.

Table 16 Password Policy

Custom Policy	You can provide a custom policy that is based on the password policy templates that are provided in the *TIBCO_HOME*`/tra/`*version*`/config/security` directory (see note below). After copying a template to another location and modifying it, click the**...** icon and load the custom policy file. The file contents are written to the domain. **Note:** Three password policy templates are provided: **DefaultPolicy** Specifies the same policy as the Default Policy radio button. **StrongPolicy** Specifies the same policy as the Restrictive Policy radio button. **NormalPolicy** In this policy, a password: • Is saved in encryption mode using 3DES-CBC algorithm with a 192-bit key. That is, SaveHashMode is set to false. • Must contain at least six characters. • Must contain at least three of the following: — One or more characters in lower case (a-z,) — One or more characters in upper case (A-Z) — One or more numeric characters (0-9) — One or more punctuation characters (,!@#$%^&*()_+ | ~-=\`{}[]:";'<>?,./)

Creating a Domain that Integrates with an LDAP Directory Server

Certain configuration information such as LDAP directory server connection search parameters and synchronization parameters must be specified when using Domain Utility to create an administration domain. These can be set at installation when creating the initial domain, or later when creating or modifying an administration domain.

After creating an administration domain that is integrated with an LDAP directory server, you cannot change the same administration domain to be a non-LDAP domain. You must create a new administration domain that does not integrate with an LDAP directory server.

You can integrate an existing domain with an LDAP directory server or modify an administration domain that uses an LDAP directory server by invoking Domain Utility and selecting the `Server Setting` category, then selecting the `LDAP Configuration` task. See Changing a Domain's Integration With an LDAP Directory Server on page 79 for details.

Working With User and Group Filters

When defining search criteria for retrieving users, groups or both from the LDAP server, you can create multiple search filters and test the search parameters before creating the domain.

The valid LDAP users that will appear in the TIBCO Administrator GUI and that can log into any TIBCO application are determined by the user filter. The valid LDAP groups that will appear as group synchronized roles in the TIBCO Administrator GUI are determined by the group filter. Group membership is limited by the user filter. This means that if a valid LDAP group contains users in its membership that are not valid based on a user filter, those users will not display in the corresponding group-synchronized role in the TIBCO Administrator GUI.

An LDAP user is a valid user if it meets any of the user filter conditions. Similarly an LDAP group is a valid group if it meets any of the group filter conditions. There is no correlation between group filter and a user filter within a set. The filters are separate, one for groups and one for users. This allows you to omit a filter in any filter set as long as there is at least one set where a user filter is specified.

If you are using Microsoft Active Directory server, there is a limit on the number of entries that can be retrieved. For information about how to manage the limit, see Searching and Active Directory Server in the *TIBCO Administrator User's Guide*.

Viewing Calls Made to the LDAP Server

Information about the calls made to the LDAP server is logged in the LDAP server's log files and can be logged in the *TIBCO_TRA_DOMAIN_HOME**domain-name*\logs\administrator.log file.

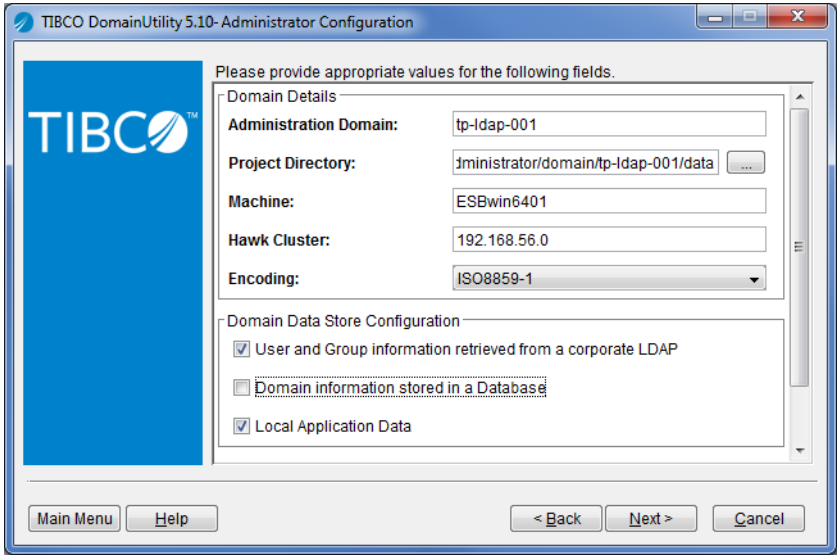
To log the calls in the administrator.log file, you must first edit the *TIBCO_TRA_DOMAIN_HOME**domain-name*\AuthorizationDomain.properties file) by setting LogDebug=true. Debug statements such as "... searchLDAP ..." will then appear in the administrator.log file.

To Create an LDAP Based Domain Using the GUI

To create an administration domain that uses LDAP users and groups:

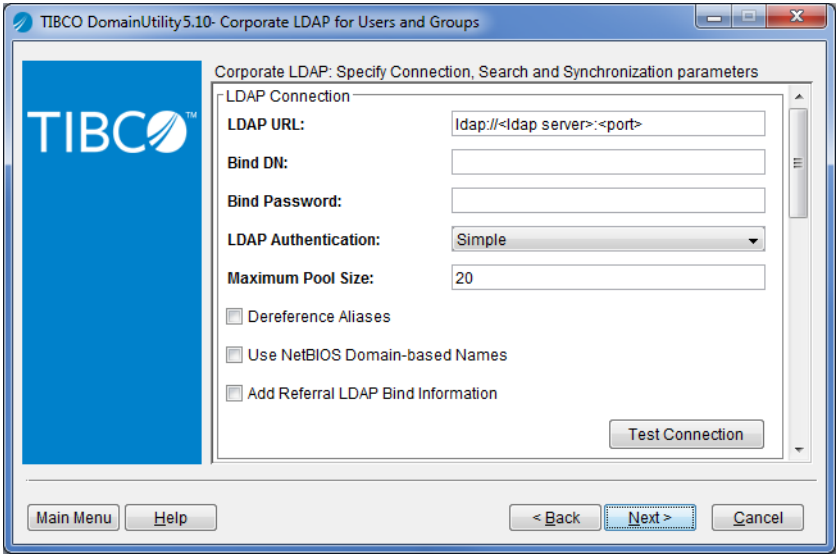
1. Start Domain Utility and click the **Next** button on the main screen.
2. Under Category, click **Domain Configuration**, then click **Create a new Administration Domain**.
3. Click **Next** and in the screen that appears, provide a name for the administration domain in Administration Domain. See Domain Details on page 28 for information about the fields that display.
4. To use TIBCO Enterprise Message Service as the transport for the domain, click **Show Advanced** and select **TIBCO EMS**. Provide values for connecting to the Enterprise Message Service server in the TIBCO EMS parameters for TIBCO Administrator panel. To use TIBCO Rendezvous as the transport, no action is necessary as Rendezvous is the default transport choice.
5. As shown next, Select User and Group information retrieved from a corporate LDAP.

Figure 3 Administrator Configuration



6. Click **Next** and, if necessary, change the values for the web server ports. In most cases, its best to accept the default settings. See Web Server Ports on page 35.
7. Click **Next** and provide the administrator credentials for the administration domain. Note that these credentials are for TIBCO Administrator, not for the LDAP directory server.
8. Click **Next** and in the screen that appears provide the LDAP connection information, search parameters and synchronization information. See LDAP Configuration Fields on page 43 for a description of these values.

Figure 4 Corporate LDAP for Users and Groups



9. Click **Next** to display a summary page where you can verify the parameters.
10. Click **Next** to create the domain. After creating the domain, start the required services that are listed in the dialog.
11. Click **Finish** to end the session.

To Create an LDAP Based Domain Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\cmdline\CreateDomain.xml`
3. Open `CreateDomain.xml` in a text editor.

   The `CreateDomain.xml` file contains sections for creating a domain that uses a repository, LDAP server, and database. Change only the LDAP server section and make sure that the LDAP server section is not commented out. The parameters for a domain that integrates with an LDAP server are explained in the following section. After changing the parameters, save the file and exit the text editor.
4. Execute the following command to apply your changes to the domain:

   `domainutilitycmd -cmdFile` *working-dir-path*`\CreateDomain.xml`

LDAP Configuration Fields

Certain LDAP settings can cause your administration server to crash at runtime. See LDAP Settings Cause the Administration Server to Crash on page 102 for more information.

Table 17 LDAP Configuration Fields

LDAP Connection	
LDAP URL	Provide the hostname and port used to connect to your corporate LDAP. The hostname can be a name or an IP address. For example, `ldap://directory.acme.com:389`
Bind DN and Bind Password	Enter the full distinguished name of the entry with which you want to log into the LDAP directory server. For example, `cn=directory manager`. TIBCO Administrator and other services in the administration domain will connect to the LDAP server with these administrator credentials. The administrator should have read access to all user and group entries within the LDAP directory. If no value is given in the `Bind Password` fields, an anonymous login into the LDAP directory server is assumed. The behavior for an anonymous login varies depending on the LDAP directory server vendor. For example, in case of Novell, an anonymous user does not have read access to much of the LDAP tree and, while the test connection may succeed, the search parameters test will fail. On the other hand, in case of the Sun ONE Directory server, anonymous login is provided with read access to the complete tree by default. Again, the defaults for an anonymous login may have been changed in your installation, and therefore it is not advisable to use anonymous login. The Bind DN provided can be an LDAP user that has only read access to LDAP. The user needs permission to: • Read LDAP user objects • Read LDAP group objects • Authenticate other users to LDAP (that is, call the LDAP authenticate API or have read access to password/credentials of LDAP user objects).

Table 17 LDAP Configuration Fields

LDAP Authentication	Set the authentication type that is accepted by your LDAP directory server. The values are `Simple` and `SSL`. If using simple authentication, the Bind DN and Bind password (in clear text) is sent to the LDAP directory server. If using SSL, see Configuring LDAP Integration With SSL Connections on page 81 for more information and additional configuration steps.
Maximum Pool Size	Set the maximum pool size for a Directory Server (LDAP) connection pool. The default maximum pool size uses a maximum of 20 connections.
Dereference Aliases	Select the check box to dereference aliases, or clear it to not dereference aliases. By default, references are not dereferenced. Aliases point to another object in a namespace. The alias contains the DN of the object to which it is pointing. When you look up an object by using the alias, the alias is dereferenced so that what is returned is the object pointed to by the alias's DN. Note that Sun ONE Directory Server does not support alias dereferencing.
Use NetBIOS Domain-based Names	If using Microsoft Active Directory with multiple domains and if users exist with the same name across the different domains, select this option. With this option selected, users will be displayed in the TIBCO Administrator GUI with names in NetBIOS format (for example, `acme_la\jsmith`). Group synchronized roles will also be created and displayed in NetBIOS format (for example, `acme_la\Human Resources`). Note that if you change this field after the administration domain has been created, all existing user profiles will be deleted. This occurs if the flag was originally selected and then cleared, or originally cleared and then selected.

Table 17 LDAP Configuration Fields

Add Referral LDAP Bind Information	An LDAP server might not store the entire Directory Information Tree (DIT). Servers can be linked together to form a distributed directory that contains the entire DIT. This is accomplished with help of server-side chaining or client-side referrals. The referral acts like a pointer that can be followed to where the desired information is stored. In case where your LDAP directory server is distributed using client-side referrals, you must specify the bind information for each of the referred LDAP directories. **Note:** You *cannot* use LDAP referral if you are using CA Directory Server as your LDAP server. When selected, the `Referral LDAP` form appears. Click the `Add` button to configure the referral LDAP bind information with an `LDAP URL`, `Bind DN` and `Bind Password`. The connection to each referral LDAP directory server can be tested. One or more bind information referrals to LDAP directories can be added. Note that you need not specify the bind information for referral LDAP directories that have the same bind information as the primary LDAP directory. You can limit the maximum number of referral hops that TIBCO applications and services should follow by setting the number in the `Maximum Referral Hops` field. This helps to avoid indefinite queries when cyclic referrals are present in LDAP directories. The referrals in LDAP (in case of Sun Java System Directory Server) must be specified correctly, that is, the attribute name and value of the referral entry be specified the same as that of the target DN. Otherwise, the group synchronized role for the groups from referral LDAP will provide correct membership information.

Table 17 LDAP Configuration Fields

	On Active Directory 2003, the following message may appear after adding a referral: `LDAPConnection.checkSearchMsg: ignoring bad referral message` If this message appears, you must set the following entries in your DNS server to point to the domain controller running the Active Directory server for the respective domains. This allows TIBCO applications and services, such as TIBCO Administrator when run on a machine of its own, to resolve the entire listed domain names through its designated DNS server. (In most cases the IT department in your organization that manages the Active Directory domains have already set it up correctly.) • DomainDnsZones.*domain* • ForestDnsZones.*domain* • *domain* Where *domain* is the domain of the domain controller, such as `acme.com` or `la.acme.com`. Refer to this article on MSDN: KCC Error Event 1567 Occurs When You Install DNS on a Windows Server 2003-Based Domain Controller (http://support.microsoft.com/default.aspx?scid=kb;en-us;813484). Note that if you connect to Global Catalog Server (port 3268) instead of Active Directory server (port 389), there are no referrals and there is no need to provided referral configuration in your administration domain.
Test Connection	Connects to the LDAP server using the connection parameters you supplied. A dialog displays, indicating success or failure.
Search Parameters and Attributes	
Vendor (provides defaults)	Click the arrow to display a popup window where you can select your LDAP vendor. This will reset the search parameters and search attributes with selected vendor defaults. Note that any search parameters added earlier will disappear, and all custom search attributes specified earlier will disappear. **Note:** If you select CA Directory Server, note that it does *not* support LDAP referral. Note also that TIBCO PortalBuilder™ does *not* support CA Directory Server.

Table 17 LDAP Configuration Fields

Add
Remove
Edit
	This allows you to add, edit or remove the search criteria for retrieving users, groups or both from the LDAP server. Click **Add** to display the search parameters dialog where you can define search criteria for users and groups. You can select the vendor for your LDAP directory server from the drop-down list to populate the fields with common values. This will reset the search parameters and search attributes with selected vendor defaults. Note that any search parameters added earlier will disappear, and all custom search attributes specified earlier will disappear.
	
	When you write a search filter, you must provide a `Base DN` value as shown next. Using the defaults for the user and group search filters, all users and groups are returned.
	
	`Base DN:` **`dc=na,dc=tibco,dc=com`**
	`User Search Filter:` **`objectclass=person`**
	`Group Search Filter:` **`objectclass=groupofuniquenames`**
	
	You can specify a user search filter and only users that have the specified attribute are returned. For example, the following returns only users that have the ProductManager attribute assigned.
	
	`Base DN:` **`dc=na,dc=tibco,dc=com`**
	`User Search Filter:`
	`(&(objectclass=person)(manager=ProductManager))`
	`Group Search Filter:` **`objectclass=groupofuniquenames`**
	
	You can specify a user and group filter and only users that have that attribute and groups that match the filter will be returned:
	
	`Base DN:` **`dc=na,dc=tibco,dc=com`**
	`User Search Filter:`
	`(&(objectclass=person)(manager=ProductManager))`
	`Group Search Filter:`
	`(&(objectclass=groupofuniquenames)(cn=TEAK*))`

User Name Attribute	Provide the LDAP attribute name that represents the user name in the LDAP directory server. For example, `uid` for the Sun ONE Directory server.
Group Name Attribute	Provide the LDAP attribute name that represents the group name in the LDAP directory server. For example, `cn` for the Sun ONE Directory server.
Group Membership Attribute	Provide the LDAP attribute that represents the group membership attribute in the LDAP directory server. The value for this attribute lists the DN for all the static group members. For example, `uniquemember` for the Sun ONE Directory server.

Table 17 LDAP Configuration Fields

Group Member URL Attribute	Provide the LDAP attribute name that identifies the dynamic group URL in the LDAP directory server. The value for attribute lists the URL to compute all the dynamic group members. For example, `memberurl` for the Sun ONE Directory server.
Use Optimistic User Membership	For both dynamic and periodic synchronization, this option is available to improve performance. This parameter is valid for LDAP directory servers with or without referrals. The parameter is only relevant when Microsoft Active Directory is used as the LDAP directory server. The membership list of an LDAP group contains users, other groups (called sub groups) and potentially other LDAP entry types such as computers or networks. The group membership list does not distinguish members and only stores the DN for each of these entries. While computing the entire group membership, TIBCO applications and services must distinguish among the entries in the membership list. The sub group entries in the list are identified by their DNs, but for other entries the application must individually retrieve the LDAP entry for each DN. This is potentially a performance issue. If the optimistic option is used, TIBCO applications and services assume that all entries that are not sub groups are valid users, and does not query the LDAP directory server. Using the optimistic option reduces the number of queries, and thus improves performance. If LDAP entries for users do not contain their user name as part of the DN, the optimistic option is useless, since individual entries must still be retrieved to obtain user names. Before using this option, you must ensure that the following are true (otherwise unpredictable results may occur): • The static membership list of any group in the LDAP directory server contains only sub-groups and valid (existent) users. If it contains other types of items such as computers or networks, the algorithm will work only if there are no users in the LDAP directory server that have the same name as any of these other items. • The static membership lists contain only users that are integrated based on user search filters specified in the LDAP setting for the administration domain. The static membership lists do not contain users that are unreachable because of LDAP referrals for which credentials are either not provided or are provided incorrectly. • The static membership lists do not contain members that are aliases of unreachable users or sub groups.

Table 17 LDAP Configuration Fields

Compute Group Hierarchy by Loading Membership	Use this option to improve performance when synchronizing with an LDAP server that contains a large number of static groups. When this checkbox is cleared, the administration server computes the group hierarchy by making a separate LDAP query to find the parent group of each group. When it is selected, the administration server loads the entire group hierarchy from the LDAP server and uses it to compute each group's parent group.
Test Search	Click to validate the search parameters you have supplied.
Synchronization Parameters	TIBCO Administrator synchronizes LDAP groups into group-synchronized roles in the domain. In addition, TIBCO applications and services authenticate users through the LDAP directory and query the LDAP directory server for group membership, users and user corporate properties.
Automatically create Roles for each Corporate Group	Select this check box to allow TIBCO Administrator to automatically synchronize LDAP groups and create roles for these in TIBCO Administration domain. Group-synchronized roles are created only for only those groups that match the search filter specified. This synchronization is repeated at intervals specified in the Synchronization Interval. Note that the groups that are synchronized can be further limited. This can be performed by manually selecting them via the Select LDAP Groups screen in the TIBCO Administrator GUI after creating this domain. If you do not set this option, you can still perform synchronization manually in the TIBCO Administrator GUI or by using the `CorpRoleSynchronizer` command line utility. See the *TIBCO Administrator User's Guide* for more information.
Synchronization Interval	This interval determines when the administration server queries the LDAP directory to discover changes in the directory's group list or group hierarchy. If groups have been added to or removed from the LDAP directory, or sub groups added to or removed from groups, the administration server makes corresponding changes to the role list and role hierarchies it maintains. The interval specified in this field sets the amount of time to expire before the administration server queries the LDAP directory server to discover changes. For example, if the time is set to 12 hours, synchronization occurs in 12 hour cycles. Changes are written to the administration domain repository. **Note:** To ensure that LDAP synchronizations happen at the same time(s) each day, specify an interval that is divisible by 24 hours.

Table 17 LDAP Configuration Fields

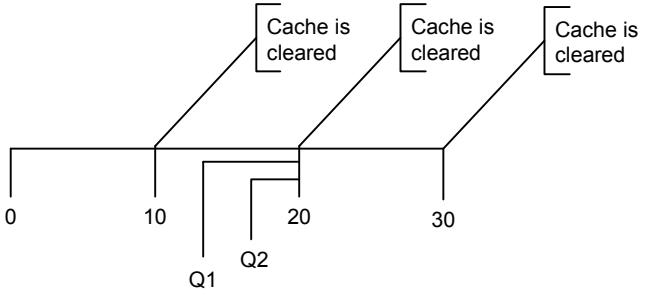
Synchronization Time of Day	Use this field to dictate a specific time that LDAP synchronization happens. The time you specify will be the time that the administration server synchronizes with the LDAP server after it starts up the first time. After the first LDAP synchronization, the time interval you specify in Synchronization Interval determines the time of the next LDAP synchronization.
Corporate User Expiration Interval	When a TIBCO application or service needs to • search for valid users, • get user properties, or • get membership of a group synchronized role, it makes a request to the LDAP directory server. These queries are made on demand and the results are cached in the application's or service's memory. It remains in memory for sometime and then this cache is cleared in order to avoid caching stale information. This interval specifies the time until this information is expired or cleared. For example, if the interval is set for 10 minutes, the TIBCO application or service's cache is cleared in 10-minute cycles. The amount of time query results persist in memory depends on when it was launched in respect to the cycle. Q1 stays in memory longer than Q2 because Q1 was launched earlier than Q2. When the 10 minute cycle repeats, the cache is cleared and Q1 and Q2 are removed from the application or service's memory. The interval is normally (much) shorter than the Synchronization Interval.  **Note:** To ensure that cached corporate users expire at the same time (s) each day, specify an interval that is divisible by 24 hours.

Table 17 LDAP Configuration Fields

Corporate User Expiration Time of Day	Use this field to dictate a specific time that the cached corporate users in memory expire (see above). The time you specify will be the time that the administration server expires cached corporate users in memory after it starts up the first time. After the first expiration, the time interval you specify in Corporate User Expiration Interval determines the time of the next expiration of cached corporate users. See also Time of Day for Expiry Parameter as described next.

Time of Day for Expiry Parameter

For Administration Domains integrated with Corporate LDAP, group memberships and user LDAP properties are retrieved from LDAP and cached in memory when required by a TIBCO Runtime Agent based application. This information expires at the schedule specified in the Corporate User Expiration Interval field in TIBCO Domain Utility. The schedule is reset automatically at midnight GMT and then proceeds using the interval given in the field. However, performance can be affected if a reset occurs during high traffic times.

You can now control when the schedule is reset with the use of the TimeOfDayForExpiry parameter. Instead of the schedule reset always occurring at midnight GMT, the reset can occur at the time given for the `TimeOfDayForExpiry` parameter.

The parameter must be specified in the `AuthorizationDomain.properties` file on each machine where TIBCO Runtime Agent is installed. Applications that use TIBCO Runtime Agent (including TIBCO Administrator) must be restarted after adding the parameter to the file. For example:

```
TimeOfDayForExpiry=2:00:00 AM EST
```

The time can be specified in any of these formats:

2:00:00 AM *time-zone*

2:00:00 AM

2:00 AM

In the case where the time zone is not specified in the parameter, it uses the default time zone of the server where the TIBCO Runtime Agent based application is running. For example:

- If `TimeofDayForExpiry` is not set and the Corporate User Expiration Interval is 24 hours, a TIBCO Runtime Agent application cache is cleared at midnight GMT (even if the application server is in some other time zone such as EST).

- If `TimeofDayForExpiry` is set to 2:00 AM EST and the Corporate User Expiration Interval is 24 hours, a TIBCO Runtime Agent application cache is cleared at 2:00 AM EST.
- If `TimeofDayForExpiry` is not set and the Corporate User Expiration Interval is 4 hours, a TIBCO Runtime Agent application cache is cleared every 4 hours counting from midnight GMT.

  (Again it is counted from Midnight GMT, even if the application server is in some other time zone such as EST).
- If `TimeofDayForExpiry` is set to 2:00 AM EST and the Corporate User Expiration Interval is 4 hours, a TIBCO Runtime Agent application cache is cleared every 4 hours counting from 2:00 AM EST.

Note that:

- `TimeOfDayForExpiry` works with the Corporate User Expiration Interval setting. Even though you can set `TimeOfDayForExpiry` to a certain time of the day, it can expire at another time of the day too, based on a Corporate User Expiration interval that is shorter than 24 hours as described in examples above.
- Avoid setting a Corporate User Expiration Interval that is not a factor of 24 hours (for example 5 hours), because that changes the expiry times on each day.
- `TimeOfDayForExpiry` does not affect the time of the synchronization process that (only) occurs in the TIBCO Administrator server and that is based on the synchronization interval that automatically creates roles for each LDAP Corporate Group.
- This feature may require further steps if the products are dependent on TIBCO Runtime Agent such as TIBCO PortalBuilder. Please refer to the specific product documentation for more information.

Creating a Domain that Uses a Database

When you create a domain with a database backend, TIBCO Administrator creates a number of database tables for the domain. If you later delete the domain, all domain-specific files are deleted, however, the database tables created when the domain was created are not deleted.

If you are already using DB2 for the previous releases of TIBCO Runtime Agent, be sure to follow the directions in the "Configuring Vendor-supplied Database Drivers" section of *TIBCO Runtime Agent Upgrading to Release 5.10* to configure your DB2 database driver properly.

The default page size for DB2 is 4k and this is not enough for creating a domain. You must create a bufferpool with 32k and then create a tablespace that uses this bufferpool. The table space must be made available to the given DB2 user.

DataDirect database drivers are not shipped since TRA 5.7. You can install TIBCO Database Drivers Supplement or configure a vendor-supplied database driver for your domains instead. You can configure the database driver during your installation of the TIBCO Runtime Agent. See *TIBCO Runtime Agent Installation* for details. See also the "Configuring Vendor-supplied Database Drivers" section of *TIBCO Runtime Agent Upgrading to Release 5.10* for detailed instructions on changing to vendor-supplied drivers for your 5.10 installations and domains.

To Create a Domain Using the GUI

1. Start Domain Utility and click the **Next** button on the main screen.
2. Under `Category`, click **Domain Configuration**, then click **Create a new Administration Domain**.
3. Click **Next** and in the screen that appears, provide a name for the administration domain in `Administration Domain`. See Add Machine Panel on page 16 for information about the fields that display.
4. Click the box next to Show Advanced and select the transport. If you select TIBCO Rendezvous, you must select the `Domain information stored in a Database` option. If you select TIBCO EMS, the option is automatically selected.
5. Review or provide values for the selected transport.
6. Click **Next** and, if necessary, change the values for the web server ports. In most cases, its best to accept the default settings. See Web Server Ports on page 35.

7. Click **Next** and provide the administrator credentials for the administration domain.
8. Click **Next** and in the screen that appears, change the values for your database connection. See Database Connection Fields on page 55 for details. Click the **Test Connection** button to verify the values.
9. Click **Next** to review the values you supplied.
10. Click **Next** to apply the values.
11. Click **Next** to display a summary page where you can verify the parameters.
12. Click **Next** to create the domain. After creating the domain, start the required services that are listed in the dialog.
13. Click **Finish** to end the session.

To Create a Domain Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory *working-dir-path*\:
   TRA_HOME\template\domainutility\cmdline\CreateDomain.xml
3. Open `CreateDomain.xml` in a text editor.

   The `CreateDomain.xml` file contains sections for creating a domain that uses a repository, LDAP server and database. Change only the database section. The parameters for a domain that uses a database are explained in the following section. After changing the parameters, save the file and exit the text editor.
4. Execute the following command to apply your changes to the domain:

   `domainutilitycmd -cmdFile` *working-dir-path*`\CreateDomain.xml`

Database Connection Fields

Table 18 Database Connection Fields

Select a driver or enter your own driver info	Choose one of the pre-specified drivers. After choosing a driver, the other fields are updated to use the appropriate format. **Note:** DataDirect database drivers are deprecated and no longer shipped in TRA 5.7.0. You should configure a vendor-supplied database driver for your domains instead. See section "Configuring Vendor-supplied Database Drivers" in *TIBCO Runtime Agent Upgrading to Release 5.10* for detailed instructions.
JDBC Driver	Provide the driver name. This field is updated to the correct value when you select or specify one in the top field.
Database URL	Provide connection information to your database. This field is displays the correct URL format for your database if you select a driver from the top field.
Username	Name of a user with appropriate privileges for the database
Password	Password for the user logging into the database.
Minimum Connections	When your application starts up, it initializes this number of connections to the database. For optimal performance, this number should equal the number of subscribers you expect to connect to the database at any one time. As you specify the minimum connections, keep in mind that these are per instance, and at startup, each instance will open its specified number of connections. Higher settings are better for application instances, but may have adverse results in the rest of the system. The correct setting is whatever the complete system can handle on a sustained basis without taxing other system resources.

Table 18 Database Connection Fields

Maximum Connections	The number of simultaneous connections cannot exceed the number set in this field. The database must be able to simultaneously handle the total maximum number of connections for all instances. Be sure that you set Max Connections to a number greater than the number for Min Connections. Otherwise you will get an error message.
Test Connection	Click this button to test the connection parameters you specified.

Adding a Secondary Server to a Domain

Use this procedure to add a secondary server to an administration domain that uses TIBCO Rendezvous as the transport. The primary server for the domain must be running. The secondary server should be added to a machine on which the primary server is *not* installed.

A secondary server can be added to a cluster environment. Before adding the server, review the information about installing a master and secondary server in a cluster in *TIBCO Runtime Agent Installing Into a Cluster*.

A secondary server can be added to an administration domain. The secondary server is equivalent to a primary server in that it has read and write permissions enabled. It can be used for load balancing and fault tolerance.

The role of a secondary server depends on the domain transport you employ:

- When you use TIBCO Rendezvous for your domain transport, secondary servers cannot deploy, undeploy, and delete applications like the primary server can.
- When you use TIBCO Enterprise Message Service for your domain transport, secondary servers function exactly like the primary server and can deploy, undeploy, and delete applications.

To Add a Secondary Server Using the GUI

Once you have added a secondary server to a domain, you *cannot* promote it to a primary server.

1. Start Domain Utility and click the **Next** button on the main screen.
2. Under `Category`, click **Domain Configuration**, then click **Add a secondary server**.
3. Click **Next** and in the screen that appears:

   Click the **Discover** button and select a domain. If a domain does not appear, select **Show Advanced** and increase the **Discover Timeout** value. The value sets the amount of time Domain Utility has to connect to the master server. If no connection is made in the specified time, the discovery operation will time out. Increase this number on slow systems and click the Discover button again.

Provide domain details. See Secondary Server Fields on page 59 for field descriptions.

Select `Show Advanced` if custom TIBCO Rendezvous parameters were specified for the master server. The same custom parameters must be defined for the secondary server.

4. Click the **Next** button. The screen that appears displays the ports used by the Web Server.
5. Click the **Next** button Provide the administration credentials that were defined when the domain was created.
6. Click the **Next** button. The screen that appears displays a summary of the values you have provided.
7. Click the **Next** button to add the secondary server to the domain. After joining the domain, the services that support the secondary server are listed. You must start each service to enable the secondary server.
8. Click **Finish** to end the session.

To Add a Secondary Server Using the Command Line Utility

Once you have added a secondary server to a domain, you *cannot* promote it to a primary server.

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\cmdline\AddSecondaryServer.xml`
3. Open `AddSecondaryServer.xml` in a text editor.

   After changing the parameters, save the file and exit the text editor.
4. Execute the following command to apply your changes to the domain:

   `domainutilitycmd -cmdFile`
   working-dir-path`\AddSecondaryServer.xml`

Secondary Server Fields

Table 19 Domain Details for Adding a Secondary Server

Domain Details	
Administration Domain	Click **Discover Domains** to choose the domain for which you wish to install a secondary server.
Project Directory	Location in which the server looks for the domain data store, for project files saved as single-file projects, and for deployment configuration files.
Machine	The name of the machine is provided in the `Machine` field and must not be changed.
Hawk Cluster	Machines are grouped in the Administrator GUI under the value provided in the `Hawk Cluster` field. If you change the default value, this machine displays in the Administrator GUI under the value you provide. The cluster name must be enclosed within quotes, if the name contains spaces.
Advanced Options	
Show Advanced	If you specified custom TIBCO Rendezvous parameters for the master server, click this check box, to specify the same custom parameters for the secondary server.
Discover Timeout	Time Domain Utility allows for connecting to the master server. If no connection is made in the specified time, the master server may be down or slow to respond and Domain Utility times out. Increase this number on slow systems.
TIBCO Rendezvous TIBCO EMS	Select the transport to use for administration domain communication. When adding a machine, you must select the transport already set for the primary domain. The fields change, depending on the transport selection. On selecting TIBCO EMS, you can edit the Hawk HMA parameters.
TIBCO Rendezvous parameters for TIBCO Administrator	

Table 19 Domain Details for Adding a Secondary Server

RV Daemon	TIBCO Rendezvous Daemon used for client-server communication. Default is tcp:7500.
RV Network	TIBCO Rendezvous network used for client-server communication. This variable need only be set on computers with more than one network interface. If specified, the TIBCO Rendezvous daemon uses that network for all outbound messages.
RV Service	TIBCO Rendezvous service used for client-server communication. The Rendezvous daemon divides the network into logical partitions. Each transport communicates on a single service. A transport can communicate only on the same service with other transports. Unless you are using a non-default TIBCO Rendezvous configuration, you should use the default (7500).
TIBCO Rendezvous parameters for TIBCO Hawk	
Hawk Daemon	TIBCO Rendezvous Daemon used for communication with TIBCO Hawk. Default is tcp:7474. See the *TIBCO Hawk Installation and Configuration* manual for details about this parameter.
Hawk Network	TIBCO Rendezvous network used for communication with TIBCO Hawk. Use the default unless you are an experienced TIBCO Rendezvous user. See the *TIBCO Hawk Installation and Configuration* manual for details about this parameter.
Hawk Service	TIBCO Rendezvous service used for communication with TIBCO Hawk. Use the default unless you are an experienced TIBCO Rendezvous user. Default is 7474. See the *TIBCO Hawk Installation and Configuration* manual for details about this parameter.
TIBCO EMS parameters for TIBCO Administrator	

Table 19 Domain Details for Adding a Secondary Server

Server URL	The URL of the TIBCO Enterprise Message Service server in the following format: `tcp://`*hostname*`:`*port*. If you have configured multiple fault tolerant servers, specify all of them here, separating them by commas. For example: `tcp://host1:7222,tcp://host2:7222`

Table 19 Domain Details for Adding a Secondary Server

Username	Specify the user account name authorized to administer the TIBCO Enterprise Message Service server. Specify a user that is a member of the `$admin` group (for example, the predefined `admin` user), or a user who has the following permissions:
	• publish, subscribe, and create permissions to the following topics:
	`com.tibco.repo.>`
	`com.tibco.pof>`
	`or`
	`com.tibco.pof.HawkConfig.>`
	`com.tibco.pof.MonitoringManagement.>`
	`com.tibco.repo.server_discovery.>`
	`com.tibco.pof.`*`domain-name`*`.> (for each domain)>`
	`com.tibco.pof.AUTH_`*`domain-name`*`.> (for each domain)`
	`com.tibco.repo.instance_mgmt.*.trustworthy_HAWK.`*`domain-name`* `(for each domain)`
	• public, subscribe, and create permissions to the `com.tibco.repo.>` queues
	Note: You must add the following topics to the *TIBCO_HOME*`/ems/bin/topics.conf` file:
	`com.tibco.pof.`*`domain-name`*`.>`
	`com.tibco.repo.server_discovery.>`
	`com.tibco.pof.AUTH_`*`domain-name`*`.>`
	`com.tibco.repo.instance_mgmt.*.trustworthy_HAWK.`*`domain-name`* (one line for each domain)
	You must also add the following queue to the *TIBCO_HOME*`/ems/bin/queues.conf` file:
	`com.tibco.repo.>`
	Note that if *domain-name*, contains the characters '.', '>' and '*', the characters must be replaced by the following strings:
	"." replaced by "2E"
	">" replaced by "3E"
	"*" replaced by "%2A"

Password	Specify the password for the user account given in the Username field.

Table 19 Domain Details for Adding a Secondary Server

Enable SSL	Select to enable Secure Sockets Layer (SSL) for use with TIBCO Enterprise Message Service. See Enabling SSL for a TIBCO Enterprise Message Service Domain on page 22 for information about using SSL.
Domain Home Paths Configuration	
TRA Domain Home	Click the**...** button and navigate to a drive shared by all nodes in the cluster. Specify the location of the TIBCO Runtime Agent domain home. For example, `C:\tibco\tra\domain`. See the *TIBCO Runtime Agent Installation* guide for information about installing TIBCO software in a cluster environment.
Administration Domain Home	Click the**...** button and navigate to a drive shared by all nodes in the cluster. Specify the location of the administration server domain home. For example, `C:\tibco\administrator\domain`.
TIBCO Rendezvous parameters for TIBCO Hawk HMA	
Use default values	Select the **Use default values** check box unless you are an experienced user.
Hawk HMA Daemon	Hawk HMA Daemon instructs the transport creation function about how and where to find the Rendezvous daemon and establish communication. The default is tcp:7474.
Hawk HMA Network	Hawk HMA Network specified, uses the specified network for all the communications.
Hawk HMA Service	Hawk HMA Service is used for client-server communication. Each transport communicates on a single service. A transport can communicate only on the same service with other transports. The default is 7475.
Cluster Group Configuration	
Machine is Logical	Select to specify that the machine is a node in a cluster.

Table 19 Domain Details for Adding a Secondary Server

Virtual IP Address	Enter the cluster virtual IP.
Symmetric Key	
Dynamic Symmetric Key	Select to use dynamically generated keys to encrypt sensitive data by default when deploying applications locally. A static key is used if this checkbox is cleared. **Note:** This option does *not* affect sensitive data in thedeployment configuration files exported using the `AppManage` utility. See *TIBCO Runtime Agent Scripting Deployment Guide* for information on how to protect sensitive data in the deployment of configuration files using an encryption password.

Table 19 Domain Details for Adding a Secondary Server

Property Files Group Name	
Authorized Group Name	This property is used to secure the `.properties` files. The specified group will be given view access to the `AuthorizationDomain.properties` and `AdministrationDomain.properties` files when these property files are created as part of domain creation. Specifying this property allows you in the specified group to use TRA utilities like `AppManage`.

Removing a Secondary Server From a Domain

Use this procedure to remove a secondary server from an administration domain that uses TIBCO Rendezvous as the transport.

The secondary administration server must be stopped before deleting it. The primary administration server and TIBCO Hawk Agent can run while the secondary server is deleted.

To Remove a Secondary Server Using the GUI

1. Start Domain Utility and click the **Next** button on the main screen.
2. Under `Category`, click **Domain Configuration**, then click **Delete an Administration Domain**.
3. Click **Next** and in the screen that appears, select an administration domain.
4. Click **Next** and in the screen that appears, provide the credentials for the domain in which the secondary server is running.
5. Click **Next** and in the screen that appears, verify that the values you have provided are correct.
6. Click **Next** to delete the secondary server.
7. Click **Finish** to end the session.

To Remove a Secondary Server Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\cmdline\DeleteDomain.xml`
3. Open `DeleteDomain.xml` in a text editor.

   After changing the parameters, save the file and exit the text editor.
4. Execute the following command on the machine on which the secondary server has been installed:

   `domainutilitycmd -cmdFile` *working-dir-path*`\DeleteDomain.xml`

Deleting a Domain

When you delete an administration domain, all domain data, including information about users and groups, deployments, and machine in the domain are lost.

Before deleting a domain, you must:

- Undeploy all deployed applications using the TIBCO Administrator GUI.
- Remove all machines (except the machine on which the administration server is running) from the administration domain using the TIBCO Administrator GUI.
- Use TIBCO Domain Utility to delete all secondary servers.
- Stop the administration server and TIBCO Hawk Agent for the domain.

If you are deleting a domain that uses a database, you must use the same database account that was used to create the domain, or an administrator account for that database.

By default, applications domains are deleted when an administration domain is deleted. To keep application domains from being deleted, select the Show Advanced check box in the Remove Administration Domain dialog and clear the Delete Application Domains check box.

On Windows 2000, after you delete a domain, the Windows Services console marks the administration server and Hawk agent services as disabled. If you do not exit the Windows Services console and then attempt to create a new domain using the name of the domain you just deleted, the domain creation will fail.

To Delete a Domain Using the GUI

1. If more than one machine belongs to the domain, you must first remove each machine from the domain or your environment will be inconsistent. See the *TIBCO Administrator User's Guide* for details.
2. Shut down the TIBCO Administration server and the TIBCO Hawk Agent for the domain. On Microsoft Windows, navigate to the Services panel and stop the two services for the domain to delete.
3. Start Domain Utility and click the **Next** button on the main screen.
4. Under `Category`, click **Domain Configuration**, then click **Delete an Administration Domain**.
5. Click **Next** and in the screen that appears, select the administration domain to delete.

6. Provide the administration domain user name and password.
7. Click **Show Advanced** and clear the check box next to **Delete Application Domains**, if you want to keep them.
8. Click **Next** and read the warning that appears.
9. Click **Next** to remove the domain.
10. Click **Finish** to end the session.

To Delete a Domain Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\cmdline\DeleteDomain.xml`
3. Open `DeleteDomain.xml` in a text editor.

   After changing the parameters, save the file and exit the text editor.
4. Execute the following command on the machine on which the secondary server has been installed:

   `domainutilitycmd -cmdFile` *working-dir-path*`\DeleteDomain.xml`

Enabling HTTPS for a Domain

Use this procedure to enable HTTPS for an administration domain that produces the following changes in behavior:

- An HTTPS connection is required between the TIBCO Administrator GUI and the administration server.
- HTTPS is added as an option for deployed applications to retrieve application data from the administration server.

This procedure does *not* enable secure communications between Hawk agents, which includes server actions like deploying, starting, and stopping applications. To secure communications between Hawk agents, use TIBCO Enterprise Message Service with SSL connections.

Self-signed certificates and certificates signed by a certificate authority (third-party certificates) are supported.

Using a self-signed certificate is only appropriate for testing purposes. You must use a third-party certificate for production systems.

To renew certificates of an existing HTTPS enabled domain, use the same procedure of enabling HTTPS again to specify the new certificates.

To Enable HTTPS Using the GUI

1. Start Domain Utility on the machine on which the administration server for the domain is running and click the **Next** button on the main screen.
2. Under `Category`, select **Domain Configuration**, then select **Enable HTTPS**.
3. Click **Next** and in the screen that appears, select an administration domain.
4. In the next screen, select an options and click **Next**. See HTTPS Fields on page 70 for field descriptions.
5. Click **Finish** to end the session.

To Enable HTTPS Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.

2. Copy the following file to your working directory:
   TRA_HOME\template\domainutility\cmdline\EnableHttpsConf.xml
3. Open EnableHttpsConf.xmlin a text editor.

   After changing the parameters, save the file and exit the text editor.
4. Execute the following command to apply your changes:

   ```
   domainutilitycmd -cmdFile
   working-dir-path\EnableHttpsConf.xml
   ```

HTTPS Fields

Table 20 HTTPS Fields for Enabling HTTPS

Generate and install a self-signed certificate	A self-signed SSL certificate is not signed by a recognized Certificate Authority. A self-signed certificate can be used for testing purposes while waiting for a signed certificate. You will be prompted for company and location information, which is then used for certificate generation. After you have completed the fields, the certificate is installed and the URL to the secure site is displayed. You must restart the Administrator server before logging into the secure site.
Generate a certificate signing request (CSR)	You will be prompted to provide information required by the signing authority. Domain Utility then generates a .csr file and a .p8 file located in *TIBCO_HOME*/administrator/domain/*domain_name*/SSL. The .csr file contains your certificate sign request and the .p8 file contains your private key. You send the .csr file to a Certificate Authority such as Entrust. The Certificate Authority returns a certificate and a CA chain certificate. You must launch Domain Utility again to install the certificates.
Install a server certificate	You will be prompted for the Server certificate and, optionally, for the Certificate Authority chain certificate. The server certificate is the certificate file you received in response to the CSR you sent to a Certificate Authority. You are also prompted for the keystore password you defined when you created the certificate. Note that the key name must be key.p8.

Certificate Signing Request Fields

Table 21 Fields for Certificate Signing Request

Email Address	Your email address.
Common Name	Name of the administration domain.
Organizational Unit	The server's organizational unit. No more than 64 characters.
Organization	The server's organization. No more than 64 characters.
City/Locality	Name of the city or locality. No more than 128 characters.
State	State for this server. This should be spelled out, but use no more than 128 characters.
Country Code	Country for this server. This must be a two-character ISO country code. See www.bcpl.net/~jspath/isocodes.html.
Validity	Number of days this certificate will be valid.
Keystore Password (Confirm Password)	Password to be used for the keystore. Must be at least six characters. Note down this password, you will later need it when installing the certificate received from the CA.

Chapter 3 Server Settings and Migration

This chapter explains how to change server settings and how to migrate from a previous release to this release.

Topics

Changing the Transport or Transport Parameters for a Domain

Use this procedure to change the TIBCO Rendezvous parameters or TIBCO Enterprise Message Service parameters used in a domain.

You must restart the administration server and secondary server (s) (if configured) after making changes to transport parameters and restart Domain Hawk Agents on every machine that has been added to the domain.

You can change the transport set for an administration domain from TIBCO Rendezvous to TIBCO Enterprise Message Service by clicking the **Switch to EMS** button. After clicking the button, properties relevant to the transport display. See Add Machine Panel on page 16 for details about the fields. This functionality is available using the command line utility.

Note that you cannot change transports if you have applications deployed using the rv, or http/https transport options. You must first undeploy these applications and redeploy them using the local transport option.

To Change Transport Parameters Using the GUI

1. Start Domain Utility on the machine on which the administration server for the domain is running and click the **Next** button on the main screen.
2. Under `Category`, select **Server Settings**, then select **Change Transport Parameters**.
3. Click **Next** and in the screen that appears, select an administration domain.
4. Provide the administrator credentials for the domain.
5. In the next screen, change the transport parameters. See Domain Details on page 28 for details.
6. Click **Next** and change the transport parameters for TIBCO Hawk.
7. Click **Next**. A summary dialog appears where you can verify that the values your provided are correct.
8. Click **Next** to change the parameters in the domain. You must restart the administration server for the changes to take effect.
9. Click **Finish** to end the session.

The EMS server must be available to change the EMS transport for a domain through Domain Utility.

To Change Transport Parameters Using the Command Line Utility

You can change transport parameters for TIBCO Rendezvous domains using the command line utility. You must use the Domain Utility GUI to change transport parameters for TIBCO Enterprise Message Service based domains.

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the `ModifyRVParameters.xml` file to your working directory. The files are located in *TRA_HOME*`\template\domainutility\cmdline.`
3. Open `ModifyRVParameters.xml` in a text editor.

   See Domain Details on page 28 for parameter descriptions. After changing the parameters, save the file and exit the text editor.
4. Execute the following command:

   ```
   domainutilitycmd -cmdFile
   working-dir-path\ModifyRVParameters.xml
   ```

EMS server must be available to change EMS transport for a domain using `domainutilitycmd.`

Changing Domain Credentials

Use this procedure to change the user name, password, or both for the domain administrator user for a domain.

You can change the original user name to another user name, the original password, or both. When changing the domain credentials, be sure to perform all the following tasks in order:

1. Log in to the TIBCO Administrator GUI and change the username or password in the Users console. See Changing Domain Administrator User Credentials in *TIBCO Administrator's Users Guide* for more information.
2. On *each* server and client machine, invoke TIBCO Domain Utility and make the same username or password change. See To Change Domain Credentials Using the GUI on page 77 or To Change Domain Credentials Using the Command Line Utility on page 78 for more information.
3. Restart all administration servers and TIBCO Hawk agents on all server and client machines.
4. Redeploy all applications with the following characteristics:
   - the application is deployed with http, https, rv, or ems transport options for application data.
   - the domain administrator's credentials are used to access the repository server for application data.

   Before you redeploy, you must manually supply the new username or password in the application's configuration panel in the Advanced tab of the Edit Application Configuration dialog for that application. See TIBCO BusinessWorks and Adapters Deployment Repository Instance in *TIBCO Administrator User's Guide* for more information.

If you are changing the original user to another username, that user must be a member of the Super Users role.

Do not change the domain credentials for a Super User if only one Super User is defined and the administration server is not running. If you do so, you will be unable to create a Super User member. Instead, make changes to the Super User role from the TIBCO Administrator GUI first, and then make the corresponding change to the domain using TIBCO Domain Utility.

Changing Password for Restrictive Password Policy

If your domain is configured to use a restrictive password policy (see Password Policy on page 36), you must use the following procedure to change the domain

administrator password.

1. Log in to TIBCO Administrator as the domain administrator using the original password.
2. In the Users console, click the domain administrator name.
3. Opposite Password, click **Change** and provide a new password. Click **OK**.
4. Log out of TIBCO Administrator.
5. Log in to TIBCO Administrator as the domain administrator. You will be prompted to provide a new password. Use the password given in step 3 as the old password. After providing the new password, log out of TIBCO Administrator.
6. Use the To Change Domain Credentials Using the GUI on page 77 procedure or the To Change Domain Credentials Using the Command Line Utility on page 78 procedure to change the domain administrator password. Note that when prompted for the old administrator password, use the original password you used in step 1. When prompted for the new password, use the new password you provided in step 5.

To Change Domain Credentials Using the GUI

1. If you are changing the password for the original user, do so first using the TIBCO Administrator GUI. If you are changing the name, that user must be a member of the Super Users role. See the *TIBCO Administrator's Users Guide* for more information.
2. Start Domain Utility on the machine on which the administration server for the domain is running and click the **Next** button on the main screen.
3. Under `Category`, select **Server Settings**, then select **Change Domain Credentials**.
4. Click **Next** and in the screen that appears, select an administration domain.
5. In the next screen, provide the old administrator username and password, then provide the new username and password.
6. Click **Next**. A summary dialog appears where you can verify that the values your provided are correct.
7. Click **Next** to change the parameters in the domain. You must restart the TIBCO Administrator administration server for the changes to take effect.
8. Click **Finish** to end the session.

To Change Domain Credentials Using the Command Line Utility

1. If you are changing the password for the original user, do so first using the TIBCO Administrator GUI. If you are changing the name, that user must be a member of the super users group. See the *TIBCO Administrator's Users Guide* for more information.
2. Create a working directory that will hold the XML file that defines configuration options.
3. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\cmdline\ChangeDomainCredentials.xml`
4. Open `ChangeDomainCredentials.xml` in a text editor.

   After changing the parameters, save the file and exit the text editor.
5. Execute the following command:

   `domainutilitycmd -cmdFile`
   working-dir-path`\ChangeDomainCredentials.xml`

Changing a Domain's Integration With an LDAP Directory Server

You can modify an administration domain's integration with an LDAP directory server. This includes configuring an existing domain with an LDAP server, as well as changing information such as the connection information, search parameters, or synchronization parameters. You must restart the administration server and secondary server (if configured) after making changes.

After integrating an administration domain with an LDAP directory server, you *cannot* change the same administration domain to be a non-LDAP domain.

To Change a Domain's Integration With LDAP Using the GUI

1. Start Domain Utility on the machine on which the administration server for the domain is running and click the **Next** button on the main screen.
2. Under `Category`, click **Server Settings**, then click **LDAP Configuration**.
3. Click **Next** and in the screen that appears, select the administration domain to change.
4. In the next screen provide the administrator credentials for the administration domain. Note that these credentials are for TIBCO Administrator, not for the LDAP directory server.
5. Click **Next** and in the screen that appears make the necessary changes. See LDAP Configuration Fields on page 43 for more information.
6. Click **Next** to display a summary page where you can verify your changes.
7. Click **Next** to apply the changes to the domain.
8. Click **Finish** to end the session.

To Change a Domain's Integration With LDAP Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TIBCO_HOME`/tra/`*version*`/template/domainutility/cmdline/ModifyLDAPConfiguration.xml`
3. Open `ModifyLDAPConfiguration.xml` in a text editor.

   The `ModifyLDAPConfiguration.xml` file allows you to specify LDAP settings for a specified administration server. Change the domain name, username,

password, and all the applicable LDAP settings. See LDAP Configuration Fields on page 43 for parameter descriptions. After changing the parameters, save the file and exit the text editor.

4. Execute the following command to apply your changes to the domain:

```
domainutilitycmd -cmdFile
working-dir-path\ModifyLDAPConfiguration.xml
```

Configuring LDAP Integration With SSL Connections

You can use SSL to secure the user and group data transmitted to your TIBCO servers and applications from the LDAP directory server. Doing so ensures privacy, integrity, and authenticity of data from the LDAP directory server.

TIBCO Domain Utility specifies SSL usage for the LDAP integration of an administration domain. Once SSL is specified for a domain's LDAP integration, the administration servers and applications depend on the security features of the JVM they run on in order to establish SSL connections with the LDAP server (and do not actively participate in establishing the SSL connections).

To configure an administration domain to connect to the LDAP directory server over SSL, you must do the following:

- Task A, Enable SSL on the LDAP Directory Server, page 81
- Task B, Configure the JRE Keystores, page 82
- Task C, Enable SSL for LDAP in TIBCO Domain Utility, page 82

Task A Enable SSL on the LDAP Directory Server

You must first enable SSL authentication on the LDAP directory server with which the administration domain is integrated. You may need to contact your IT department in your organization that manages your LDAP servers. This requires installing a valid server certificate and CA trust certificate from a certificate authority on the LDAP directory server. Go to one of the following links for information on enabling SSL on your LDAP directory server:

For **Microsoft Active Directory 2000**:
http://support.microsoft.com/default.aspx?scid=kb;en-us;247078#1

For **Microsoft Active Directory 2003**:
http://support.microsoft.com/kb/321051

For **Sun ONE Directory Server 5.1**:
http://docs.sun.com/source/816-5606-10/ssl.htm#996824

For **Sun ONE Directory Server 5.2**:
http://docs.sun.com/source/816-6698-10/ssl.html#14365

For **Novell eDirectory 8.7.3**:
http://www.novell.com/documentation/edir873/index.html?treetitl.html

Task B Configure the JRE Keystores

Next, you must import the CA trust certificate (the signing certificate of your LDAP server certificate) into the keystores of all JREs that are used by software or applications that perform user authentication. This includes JREs for all primary and secondary servers, as well as for BusinessWorks processes that perform basic authentication. The best thing to do is to perform this task on all TIBCO JREs in all server and client machines in your administration domain.

TIBCO JRE keystores already contain certificates from well-known certificate authorities such as Verisign, Thawte and Entrust. You can skip this task if your LDAP server certificate is issued by one of these well-known certificate authorities.

Follow the instructions below to import the CA trust certificate of LDAP server certificate into each applicable JRE keystore:

1. In the command prompt, change to *TIBCO_HOME*`/tibcojre/`*version*`/bin`.
2. Use the following command to import the CA trust certificate into the default JRE keystore. (You may specify any value for *alias_name*.)

   `keytool -import -alias` *alias_name*`-keystore`
   `TIBCO_HOME/tibcojre/version/lib/security/cacerts`
   `-trustcacerts -file` *CA_trust_certificate_file_path*
3. When prompted, type **`changeit`** for the keystore password (unless you have changed it previously).

Task C Enable SSL for LDAP in TIBCO Domain Utility

Follow the instructions in Changing a Domain's Integration With an LDAP Directory Server on page 79 to modify LDAP configuration for your administration domain in TIBCO Domain Utility.

- Specify the LDAP server's enabled SSL port in the **LDAP URL** field.
- Select **SSL** in the LDAP Authentication drop-down list.

Changing the Database for a Domain

Use this procedure to change the database used by an administration domain to a different database. The domain must have been originally created using a database as the domain data store.

You must:

- Use the database migration tools supplied by your database vendor to migrate the tables used by TIBCO Administrator to the new database. Do this before completing this procedure.
- Use the procedure in this section to identify the new database for the administration domain on *both* the server and client machines. Domain Utility is used to change values for the database connection.
- Restart the primary administration server, secondary administration server (if configured), and all client Hawk agents after making the changes.
- Log in to the TIBCO Administrator GUI and update the database configuration for each application domain in the administration domain (if applicable).

To Change the Database Using the GUI

1. Start Domain Utility on the machine on which the administration server for the domain is running and click the **Next** button on the main screen.
2. Under `Category`, click **Server Settings**, then click **Database Configuration**.
3. Click **Next** and in the screen that appears, select the administration domain to change.
4. In the next screen change the values for your database connection. Click the **Test Connection** button to verify the values. See Database Connection Fields on page 55 for details.
5. Click **Next** to review the values you supplied.
6. Click **Next** to apply the values.
7. Click **Finish** to end the session.

To Change the Database Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.

2. Copy the following file to your working directory:
   TIBCO_HOME`/tra/`*version*`/template/domainutility/cmdline/ModifyDBConfiguration.xml`
3. Open `ModifyDBConfiguration.xml` in a text editor.

   The `ModifyDBConfiguration.xml` file allows you to specify the values for your database connection. See Database Connection Fields on page 55 for details. After changing the parameters, save the file and exit the text editor.
4. Execute the following command to apply your changes to the domain:

   ```
   domainutilitycmd -cmdFile
   working-dir-path\ModifyDBConfiguration.xml
   ```

Changing the Max Deployment Revision Value

Use this procedure to change the default number of application revisions to keep in the revision history for each deployed application.

You must restart the administration server after making changes to the Max Deployment Revision Value.

To Change the Max Deployment Revision Value Using the GUI

1. Start Domain Utility on the machine on which the administration server for the domain is running and click the **Next** button on the main screen.
2. Under `Category`, click **Server Settings**, then click **Miscellaneous**.
3. Click **Next** and in the screen that appears, select the administration domain to change.
4. Provide the administrator credentials for the domain.
5. In the next screen, change the Max Deployment Revision Value. See Domain Details on page 28 for details.
6. Click **Next** to review the value you supplied.
7. Click **Next** to apply the values.
8. Click **Exit** to end the session.

To Change the Max Deployment Revision Value Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TIBCO_HOME`/tra/`*version*`/template/domainutility/cmdline/Miscellaneous.xml`
3. Open `Miscellaneous.xml` in a text editor.

   The Miscellaneous.xml file allows you to specify the Max Deployment Revision Value. See Domain Details on page 28 for details. After changing the parameters, save the file and exit the text editor.
4. Execute the following command to apply your changes to the domain:
   `domainutilitycmd -cmdFile` *working-dir-path*`\Miscellaneous.xml -domain` <*domainName*> `-user` <*userName*> `-pw` <*password*>

Upgrading a Domain

After you have upgraded a release 5.x administration domain to release 5.10, you must use TIBCO Administrator 5.10 to administer the domain. See *TIBCO Runtime Agent Upgrading to Release 5.10* guide for more information. The guide is part of the TIBCO Runtime Agent documentation set.

After upgrading an administration domain, you cannot revert back to the previous release.

When upgrading a domain on a machine that has an Administrator server for that domain, both the Administrator server and the Hawk Agent for the domain will be upgraded to the latest code. If the machine does not contain an Administrator server for the domain being upgraded, then only the Hawk Agent will be upgraded. No other domains will be touched and no change will happen to the deployed applications.

If you are using EMS transport for your domain, you need to set EMS client libraries in tra filefor the product. Run traUpgradeManager with -ems option to update the tibcoadmin_domainname.tra and hawkagent_domainname.tra files in case the domain uses EMS transport. The traUpgradeManager utility will update the path and classpath in the tra files by adding the location of the EMS libraries.

traUpgradeManager -path c:/tibco/tra/domain/<domain name> -ems c:/tibco/ems/8.0

traUpgradeManager -path c:/tibco/administrator/domain/<domain name> -ems c:/tibco/ems/8.0

To Upgrade a 5.x Domain

1. Start Domain Utility on the machine on which the administration server for the domain is running and click the **Next** button on the main screen.
2. Under **Category**, click **Migration**, then click **Upgrade Domain to 5.10**.
3. Click **Next** and on the displayed screen, select the administration domains to migrate to 5.10.
4. In the next screen review the listed domain (s).
5. Click **Next** to start the upgrade. If errors occur, they are logged to the *TIBCO_TRA_DOMAIN_HOME**domain-name*\`logs` folder.
6. Click **Finish** to end the session.

Chapter 4 EMS Server Plugin

This chapter explains how to register TIBCO Enterprise Message Service servers and servlet engines.

Topics

Adding an EMS Server to a Domain

Use this procedure to create a new mapping for a TIBCO Enterprise Message Service server so that it can be administered using the TIBCO Administrator GUI as part of an administration domain.

TIBCO Domain Utility can verify the connection to the TIBCO Enterprise Message Service server only if Domain Utility is running on the machine on which the EMS server is installed. Before adding an EMS server to a domain:

- Start the EMS server using the *TIBCO_HOME*`\ems\bin\tibemsd` command.
- Using the `tibemsadmin` command-line utility, connect to the server and establish an EMS administration user name and password.

When adding an EMS Server to administration domain in a 64-bit environment, TIBCO Domain Utility must be enabled to use 64-bit libraries. See the *TIBCO Runtime Agent Installation Guide* for information about enabling TIBCO applications to run in 64-bit mode.

To Add an EMS Server Using the GUI

1. Start Domain Utility on the machine on which the EMS server to be added is running and click the **Next** button on the main screen.
2. Under `Category`, click **TIBCO EMS Plugin**, then click **Add TIBCO EMS Server**.
3. Click **Next** and in the screen that appears, select an administration domain.
4. Provide the Administrator credentials for the domain and click **Next**.
5. The displayed screen describes the machine on which the TIBCO Enterprise Message Service software is installed. See EMS Server Machine Fields on page 89 for field descriptions. Change these values if required and click **Next**.
6. Provide information about the TIBCO Enterprise Message Service server. See EMS Server Fields on page 90 for field descriptions. Select **Secure (SSL) Connection** if required. Click **Next**.

SSL is a protocol for transmitting encrypted data over the Internet or an internal network. SSL works by using public and private keys to encrypt data that is transferred over the SSL connection.

7. Provide values in the field for configuring the SSL connection. Click **Next**. A summary of the values you provided is displayed. Click the **Test** button to verify the values.
8. Click **Next** to add the server to the domain.
9. Click **Finish** to end the session.

To Add an EMS Server Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory *working-dir-path*\:
   TRA_HOME\template\domainutility\cmdline\AddJMSServer.xml
3. Open `AddJMSServer.xml` in a text editor.

   The parameters are explained in the next section. After changing the parameters, save the file and exit the text editor.
4. Execute the following command to apply your changes to the domain:

   `domainutilitycmd -cmdFile` *working-dir-path*`\AddJMSServer.xml`

EMS Server Machine Fields

Table 22 Fields for Adding EMS Server Machine

Machine Name	Provide the machine name on which the TIBCO Enterprise Message Service server is running. This must be the actual name and cannot be the IP address or an alias to the machine.
Cluster	The name of the container in which the Hawk agent will appear in the display by default. The display will create the container if it does not already exist. This allows for grouping of multiple agents. The default name for the container is the IP subnet address. The cluster name must be enclosed within quotes, if the name contains spaces.
OS Name	Operating system.
OS Version	Operating system version.

EMS Server Fields

Table 23 Fields for Adding EMS Server

Version	Provide the version number of the TIBCO Enterprise Message Service server you are installing. This version number will be displayed in the TIBCO Administrator GUI.
Executable File	Provide the full path to the TIBCO Enterprise Message Service server executable (`tibemsd`). For most Microsoft Windows systems, this path name is *TIBCO_HOME*`/ems/bin/tibemsd.exe`. Note that forward slashes are required.
Configuration File	Provide the full path of the server instance's configuration file. The location of the working directory is inferred from the location of the configuration file. The configuration file `tibemsd.conf` locates in the EMS configuration directory that is defined during the installation of the specific version of TIBCO Enterprise Service. For example, the configuration file defaults to `TIBCO_HOME/ems/6.0/bin/tibemsd.exe` for a default installation of TIBCO Enterprise Message Service 6.0.0. Refer to *TIBCO Enterprise Message Service Installation* for the default location of `tibemsd.conf` on Unix and Windows platforms.
User Name	Specify the user account name authorized to administer the TIBCO Enterprise Message Service server.
Password	Specify the password for the user account given in User Name.
Port	Provide the port number on which the administration server is sending and receiving messages. Default is 7222.
Secure (SSL) Connection	Select the **Secure (SSL) Connection** check box to secure the communication between networks.

SSL Parameters

The following parameters are set when configuring SSL for a domain that uses an Enterprise Message Service server.

Table 24 Fields for Adding SSL Connection

Do Not Verify Host	Specifies whether the client should verify the server's certificate. When cleared, the client should verify the server's certificate. This is recommended. When selected, the client establishes secure communication with the server, but does not verify the server's identity.
Trusted	A list of CA certificates to trust as issuers of server certificates. Supply only CA root certificates.
Identity	The client's digital certificate. Supply a certificate in either the PEM or PKCS#12 format. You must also supply a private key file in the **Private Key** field if you supply a PEM-formatted certificate here.
Private Key	The name and location of the client's private key file. This key must be in the PKCS#8 format.
Password	The password for the client's private key.
Do Not Verify Hostname	Specifies whether the client should verify the name in the **CN** field of the server's certificate. When cleared, the client should verify the name of the connected host or the name specified in the Expected Hostname field against the value in the server's certificate. If the names do not match, the connection is rejected. When selected, the client establishes secure communication with the server, but does not verify the server's name.
Expected Hostname	The name the client expects in the **CN** field of the server's certificate. If this parameter is not set, the expected name is the hostname of the server. The value of this parameter is used when the `Do Not Verify Hostname` parameter is cleared.

Table 24 Fields for Adding SSL Connection

Cipher Suite Names	Specifies the cipher suites that the client can use. Supply a list of cipher names by clicking **Add** and selecting from the pull down menu that is displayed. Remove an entry from the list by selecting the entry and clicking **Remove**. Make an in place change to the list by selecting an entry and clicking **Edit**. Select a replacement entry from the pull down menu that appears. For more information, see "Specifying Cipher Suites" in the *TIBCO Enterprise Message Service User's Guide*.

Removing an EMS Server from a Domain

This procedure removes the mappings of a registered TIBCO Enterprise Message Service server from an administration domain.

To Remove an EMS Server Using the GUI

1. Start Domain Utility on the machine on which the EMS server to be removed is running, and click the **Next** button on the main screen.
2. Under `Category`, click **TIBCO EMS Plugin**, then click **Remove TIBCO EMS Server**.
3. Click **Next** and in the screen that appears, select an administration domain.
4. Provide the administration credentials that were defined when the domain was created.
5. Click **Next** and, under `Remove from Domain`, select the server to remove from the list.
6. Click **Next** to review your selections.
7. Click **Next** to unregister the selected EMS server.
8. Click **Finish** to end the session.

To Remove an EMS Server Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\cmdline\RemoveJMSServer.xml`
3. Open `RemoveJMSServer.xml` in a text editor.

   After changing the parameters, save the file and exit the text editor.
4. Execute the following command to apply your changes to the domain:

   ```
   domainutilitycmd -cmdFile
   working-dir-path\RemoveJMSServer.xml
   ```

Updating an EMS Server in a Domain

Use this procedure to change the mappings of a registered TIBCO Enterprise Message Service server as part of a administration domain.

You cannot change the machine on which the administration server is deployed. Instead use Adding an EMS Server to a Domain on page 88

To Update an EMS Server Using the GUI

1. Start Domain Utility on the machine on which the EMS server to be updated is running and click the **Next** button on the main screen.
2. Under `Category`, click **TIBCO EMS Plugin**, then click **Update TIBCO EMS Server**.
3. Click **Next** and in the screen that appears, select an administration domain.
4. Provide the administration credentials that were defined when the domain was created.
5. Click **Next** and, under `Update in Domain`, select the server to update.
6. Change the values. See EMS Server Machine Fields on page 89 and EMS Server Fields on page 90 for a description of each value.
7. Click **Next** to review and test the values you supplied. If the TIBCO Enterprise Message Service server is running on the same machine as Domain Utility, you can use the **Test** button to verify the connection.
8. Click **Next** to apply the values.
9. Click **Finish** to end the session.

To Update an EMS Server Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\cmdline\UpdateJMSServer.xml`
3. Open `UpdateJMSServer.xml` in a text editor.

   See EMS Server Machine Fields on page 89 and EMS Server Fields on page 90 for parameter descriptions. After changing the parameters, save the file and exit the text editor.

4. Execute the following command to apply your changes to the domain:

   ```
   domainutilitycmd -cmdFile
   working-dir-path\UpdateJMSServer.xml
   ```

Adding or Updating a Servlet Engine to a Domain

Use this procedure to add or update a servlet engine to a selected administration domain.

A servlet engine plug-in is not included in TIBCO Administrator. Other TIBCO products, such as TIBCO PortalBuilder, TIBCO BusinessWorks Workflow and TIBCO BusinessFactor may include a servlet engine plug-in, which would be installed in TIBCO Administrator using these steps.

To Add a Servlet Engine Using the GUI

1. Start Domain Utility on the machine on which the administration server for the domain is running and click the **Next** button on the main screen.
2. Under `Category`, click **Servlet Engine Plugin**, then click **Add Servlet Engine**.
3. Click **Next** and in the screen that appears, select an administration domain.
4. Provide the administration credentials that were defined when the domain was created.
5. Click **Next** and select the servlet engine vendor for deploying web applications. The actual servlet engine instance should be pre-configured using the respective vendor's administration tool.
6. Click **Next** and provide values for the servlet engine. This typically includes the installation root directory and the location of the servlet's configuration file. Other information may be required, depending on the servlet.
7. Click **Next** and provide the administration credentials for the servlet.
8. Click **Next** to review the values you supplied.
9. Click **Next** to add the servlet engine to the domain.
10. Click **Finish** to end the session.

To Add a Servlet Engine Using the Command-Line Utility

1. Create a working directory that holds the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\add_<`*app server*`>_servlet_engine_task.xml`

Select an appropriate `add_<app server>_servlet_engine_task.xml` from the following:

- `add_generic_j2ee_servlet_engine_task.xml`
- `add_jrun_servlet_engine_task.xml`
- `add_sun_java_system_web_server_task.xml`
- `add_tomcat_servlet_engine_task.xml`
- `add_weblogic_servlet_engine_task.xml`

3. Open `add_<app server>_servlet_engine_task.xml` in a text editor.

   After changing the parameters, save the file and exit the text editor.

4. Execute the following command to apply your changes to the domain:

   ```
   domainutilitycmd -cmdFile
   working-dir-path\add_<app server>_servlet_engine_task.xml
   ```

To Update a Servlet Engine Using the Command Line Utility

1. Create a working directory that will hold the XML file that defines configuration options.
2. Copy the following file to your working directory:
   TRA_HOME`\template\domainutility\update_servlet_engine_task.xml`
3. Open `update_servlet_engine_task.xml` in a text editor.

   After changing the parameters, save the file and exit the text editor.

4. Execute the following command to apply your changes to the domain:

   ```
   domainutilitycmd -cmdFile
   working-dir-path\update_servlet_engine_task.xml
   ```

Removing a Servlet Engine from a Domain

Use this procedure to remove a servlet engine from a selected administration domain.

To Remove a Servlet Engine Using the GUI

1. Start Domain Utility on the machine on which the administration server for the domain is running and click the **Next** button on the main screen.
2. Under `Category`, click **Servlet Engine Plugin**, then click **Remove Servlet Engine**.
3. Click **Next** and in the screen that appears, select an administration domain.
4. Provide the administration credentials that were defined when the domain was created.
5. Click **Next** and select the servlet engine to remove.
6. Click **Next** to remove the servlet engine.
7. Click **Finish** to end the session.

Appendix A Troubleshooting

This appendix list trouble shooting information related to TIBCO Domain Utility.

Topics

Domain Configuration Category Does Not Display

On Microsoft Windows, if the Domain Configuration category does not display in TIBCO Domain Utility, do the following:

1. Using a text editor, open the `domainutility.tra` file. The file is located in the *TRA_HOME*`\bin` folder.
2. Add the **-DdebugCategories=true** property to the file.
3. Start TIBCO Domain Utility.
4. Open the `domainutility.log` file. By default, the file is located in the *TRA_HOME*`\logs` folder.

If no product information is logged in the file, your Windows registry is very likely corrupt and consequently no information about TIBCO products is available using TIBCO Installer APIs. The work around is to uninstall and reinstall all TIBCO products on the machine.

Hawk Agent Does Not Start With Updated PATH Values On Windows Machines

If you make changes to the PATH system variable, the Hawk agents for existing domains will continue to use the old PATH value when restarted. To reflect the PATH variable changes in the Hawk agents for existing domains, you must uninstall and reinstall them as Windows services. You can use the Wrapper utility provided in the *TIBCO_HOME*/tra/*version*/bin directory.

Follow the instructions below for each existing domain:

1. In a command prompt, change to *TIBCO_HOME*/tra/*version*/bin.
2. Execute the following command to uninstall the domain's Hawk agent:

   ```
   wrap --propFile
   TIBCO_HOME/tra/domain/domain-name/tibhawk_domain-name.tra
   --uninstall
   ```

   For example:

   ```
   wrap --propFile C:\tibco\tra\domain\sample\tibhawk_sample.tra
   --uninstall
   ```

3. Execute the following command to install the domain's Hawk agent again:

   ```
   wrap --propFile
   TIBCO_HOME/tra/domain/domain-name/tibhawk_domain-name.tra
   --install
   ```

   For example:

   ```
   wrap --propFile C:\tibco\tra\domain\sample\tibhawk_sample.tra
   --install
   ```

LDAP Settings Cause the Administration Server to Crash

Making the following LDAP settings for a domain in TIBCO Domain Utility can cause your administration server to crash:

- clearing the **Automatically create Roles for each Corporate Group** checkbox
- selecting **Never** in Synchronization Interval
- selecting **Never** in Corporate User Expiration Interval

This particular combination is *not* supported. Follow the instructions below to change your domain's LDAP settings:

1. Go to the LDAP Configuration pane in TIBCO Domain Utility by following the instructions in Changing a Domain's Integration With an LDAP Directory Server on page 79.
2. In the LDAP Configuration pane for your administration domain in TIBCO Domain Utility, select the **Automatically create Roles for each Corporate Group** checkbox.
3. Change Synchronization Interval to **12 hours**.
4. Change Corporate User Expiration Interval to **10 minutes** or longer.
5. Clear the **Automatically create Roles for each Corporate Group** checkbox.
6. Restart the administration server.

Index

A

C

D

E

H

L

M

O

P

R

S

T

U

V

W