# TIBCO® Enterprise Administrator SDK Installation Guide

*Software Release 2.2.0*
*March 2015*

Two-Second Advantage®

## Important Information

# Contents

# Figures

# TIBCO Documentation and Support Services

All TIBCO documentation is available on the TIBCO Documentation site, which can be found here:

https://docs.tibco.com

### Product-Specific Documentation

Documentation for TIBCO products is not bundled with the software. Instead, it is available on the TIBCO Documentation site. To directly access documentation for this product, double-click one of the following file depending upon the variant of TIBCO Enterprise Administrator you are using:

For TIBCO Enterprise Administrator SDK use: *TIBCO_HOME*\release_notes\TIB_tea-sdk_<version>_docinfo.html.

For TIBCO Enterprise Administrator use:*TIBCO_HOME*\release_notes\TIB_tea_<version>_docinfo.html

The following documents can be found in the TIBCO Documentation Library for TIBCO® Enterprise Administrator:

- *TIBCO® Enterprise Administrator Release Notes*
- *TIBCO® Enterprise Administrator Installation*
- *TIBCO® Enterprise Administrator User's Guide*
- *TIBCO® Enterprise Administrator Developer's Guide*
- *TIBCO® Enterprise Administrator Agent for TIBCO Enterprise Message Service™ Guide*
- *TIBCO® Enterprise Administrator Agent for TIBCO® Security Server Guide*

### 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.

### 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:

https://www.tibcommunity.com

# Installation Overview

TIBCO® Enterprise Administrator comprises the TIBCO Enterprise Administrator server, a web user interface for the server, the shell interface, Python scripts, and an agent library to build your own agents. In addition to this, the TIBCO Enterprise Administrator also installs the agent for TIBCO Enterprise Message Service™ and TIBCO® Security Server.

# Preparing for Installation

Before downloading and extracting the installation package, ensure that the system meets all the prerequisites and decide on the installation environment and folder.

- *TIBCO_HOME* is the top-level installation directory for TIBCO products.
- *TIBCO_HOME* is referred to as the installation environment.

Installation environments isolate software installations; a software installed into an installation environment does not automatically access components in other environments. An installation environment consists of

- A name that identifies the environment and it is appended to the name of the Windows services created by the installer. It is a component of the path to the product in the **Windows Start > All Programs** menu.
- A folder that contains the installed software. When you install, you can choose a new installation environment or an existing installation environment.

If a previous installation of a TIBCO product did not use the TIBCO Universal Installer, the TIBCO Universal Installer does not detect the folder it uses as an installation environment folder. If you want to use the existing location as the installation folder, create a new installation environment and choose the folder where the other products exist.

# Installation Requirements

Before you can run the installer on your Microsoft Windows or Linux system, you must log in as a user with appropriate permissions, and your system must meet the hardware and software requirements.

If you plan on installing in an existing installation environment, stop all processes that are using Java from *TIBCO_HOME*.

### Installation Account Requirements

To install on Microsoft Windows or on UNIX, you must have the appropriate privileges. The privileges differ for different platforms.

- **Microsoft Windows** - Only users with administrator privileges can install the TIBCO Enterprise Administrator. If you do not have administrator privileges, the installer exits. To install the product on a network drive, ensure that the account used for installation has the permission to access the network drive.

  On UAT enabled Windows platforms, non-default administrators may encounter permission issues in certain circumstances. To avoid permission issues, start TIBCO Universal Installer, with the **Run as Administrator** option.

- **UNIX** - Any type of user—regular (non-root) user and super-user (root)—can install the product. A graphic environment such as CDE or X Windows is required to run the installer in the GUI mode.

## Hardware Requirements

Installation requires a substantial amount of system memory and disk space. Review the system memory and disk space requirements before you start installation.

### System Memory

A minimum of 512 MB of physical memory is required.

### Disk Space

The installer requires space in the temporary directory before installation, and additional space in the temporary directory for running the installer. You must also make sure that the directory you want to use as the installation environment (*TIBCO_HOME*) directory has sufficient space.

While installing, avoid running other processes that consume disk space in the installation environment directory. If another process consumes disk space while the installer is copying the files, the installer might fail and display a failure message.

| Directory | Disk Space Requirement |
|---|---|
| Temporary directory before installation | Before you start the installation process, extract the contents of the installation archive to a temporary directory. The installer files consume up to 100 MB of disk space. |

| Directory | Disk Space Requirement |
|---|---|
| Temporary directory during installation | The installer requires at least 100 MB of free space in the temporary directory. On Microsoft Windows, the default temporary directory location is `%SystemDrive%:\Documents and Settings\`*`user_name`*`\Local Settings\Temp`.<br><br>If your system does not have sufficient free disk space in the default temporary directory, you can use the `is:tempdir` option to run the installer with a different temporary directory. For example:<br><br>**`TIBCOUniversalInstaller`***`Platform`* `-is:tempdir \new_tmp`<br><br>where `\new_tmp` has sufficient free disk space. |
| Installation environment directory | The installer calculates the disk space required in the installation environment directory for the selected components. The calculation is done before the actual installation (copying of files to system) begins. The installer proceeds only if sufficient free disk space is available in the installation environment directory. TIBCO Enterprise Administrator might consume 200 MB of free space under *TIBCO_HOME*. |

## Software Requirements

Your system must meet the software requirements before you run the installer. Some software is required, and others optional.

Before you run the installer, you must make sure you are running on a supported platform. See the `readme` file for information about the supported operating system platforms and versions.

| Software | Description |
|---|---|
| Java | Required. Install Java 1.7.x. |
| Web Browser | Required to run the TIBCO Enterprise Administrator server UI. Refer to the `readme` file for details. |
| TIBCO Hawk | Optional. Install TIBCO Hawk 5.1.1. |
| Python | Optional. Install Python 2.7 or later. |

# Installation

Install TIBCO products with TIBCO Universal Installer. The installer runs on multiple platforms. You can run the installer in the GUI mode, console mode, or silent mode.

## Installing in the GUI Mode

When you run the installer in the GUI mode, the installer prompts you for information about the installation environment, and allows other customizations.

### Procedure

1. Open the physical media or download the package.
   a) Extract the contents of the package to a temporary directory.
   b) Navigate to the temporary directory.
2. Run TIBCOUniversalInstaller. You can do so in one of the following ways:
   - Double-click the installer icon.
   - On the command prompt, provide the absolute path of the installer file without specifying any options. The installer defaults to the GUI mode.
3. On the Welcome dialog, click the **Next** button.
4. Read through the license text when the License Agreement dialog appears, select the **I Accept The Terms of The License Agreement** radio button and then click the **Next** button.
5. In the TIBCO Installation Home dialog, select an installation environment.
   An installation environment isolates product installations. A product installed into an installation environment does not access components in other installation environments. An installation environment consists of a name and path. You can specify a new environment or an existing environment.
   a) **Create A New TIBCO_HOME**: To install the product into a new installation environment, specify the following properties:
      - **Directory**: The directory into which the product is installed. Type a path or click **Browse** to specify the path or accept the default location. The path cannot contain special characters such as "*", "#", "?", ">", "<", "%", "&", "$", "`", or "|". The path cannot be the same as the path of an existing environment.
      - **Name**: Identifies the installation environment. The name cannot contain special characters such as "*", "?", ">", "<", ":", "|", "/", "\", or quotation marks("). The name is appended to the name of the Windows services created by the installer. It is a component of the path to the product in the **Windows Start > All Programs** menu.
   b) **Use An Existing TIBCO_HOME**: To install the product into an existing installation environment, select the environment from the drop-down list. In this case, select **Use An Existing TIBCO_HOME** to install this product into the *TIBCO_HOME* directory where the TIBCO products are installed.

      You can install TIBCO Enterprise Administrator in an existing *HAWK_HOME* or *TRA_HOME*.
   c) Click the **Next** button.
6. By default, TIBCO Universal Installer selects the Typical installation profile. To customize the profile feature settings, select the **Customize Installation** check box and use the feature tree on the right. Click the **Next** button. The following components can be installed if you select custom installation:

| Installation Profile | Components Installed |
|---|---|
| TIBCO Enterprise Administrator SDK | The TIBCO Enterprise Administrator server component is installed. Along with the server, the Web UI, the command-line interface, the Python scripts, the agent library to build your own agents, the agent for TIBCO Enterprise Message Service, and the agent for TIBCO Security Server are installed. |
| TIBCO Hawk Agent | The Hawk agent is installed.<br>A Hawk agent is an autonomous process that resides on each computer that monitors TIBCO applications on the computer.<br>The TIBCO Hawk agent operates autonomously and is active whenever the operating system it monitors is active. The Hawk agent uses a set of rules, called rulebases, to configure system management, status, and automation tasks. The Hawk agent monitors conditions on its local machine and send alerts over the network only when problems are detected. |

7. Select the folder that must be used as the TIBCO configuration folder (*TIBCO_CONFIG_HOME*). Ensure that the folder you use is not already being used by another TIBCO product. The subfolder, `tibco\cfgmgmt\tea` is appended to the path. Click **Next**.

If you are upgrading, the installer stores a backup of the `logging.xml` and `tea.conf` files in the *<TIBCO_CONFIG_HOME>*`\tibco\cfgmgmt\tea\conf` folder. They are stored as `tea_backup_<timestamp>_<meridiem_indicator>.conf` and `logging_backup_<timestamp>_<meridiem_indicator>.xml`. The `meridiem_indicator` can be `AM` or `PM`. To use the existing configuration properties with new version of TIBCO Enterprise Administrator, ensure that you rename them back to `tea.conf` and `logging.xml`.

8. Point to the existing location of the Java directory and click **Next**. TIBCO Enterprise Administrator supports Java 8.

If you have selected TIBCO Hawk Agent as one of the components to be installed, and you do not have TIBCO Rendezvous on the selected TIBCO_HOME, you will be prompted that you install TIBCO Rendezvous separately. The version of TIBCO Rendezvous installed is dependent on the installed JRE version.

| Installed JRE Version | TIBCO Rendezvous Version |
|---|---|
| 1.6 | 8.1.1 |
| 1.7 | 8.4.0 |

If you have selected TIBCO Hawk Agent one of the components to be installed, and if the installer does not detect an EMS_HOME in the TIBCO_HOME selected, you will be prompted to install TIBCO Enterprise Message Service separately. The version of TIBCO Enterprise Message Service installed is dependent on the installed JRE version.

| Installed JRE Version | TIBCO Enterprise Message Service Version |
|---|---|
| 1.6 | 6.0.0 |
| 1.7 | 6.3.0 |

9. The TIBCO Enterprise Administrator can be started as an NT service. Specify one of the following startup types:

    1. **Manual**
    2. **Automatic**
    3. **Automatic (Delayed Start)**
    4. **Disabled**

    Click **Next**.

10. Verify the list of products selected to install in the Pre-Install Summary window. Click the **Install** button to start the installation process.
11. Review the information listed in the Post-Install Summary window. Click the **Finish** button to complete the installation process and exit the universal installer.

### Result

**Components that Get Installed:**

The installer installs the following:

1. TIBCO Enterprise Administrator server
2. Agent library
3. Shell interface
4. Python scripts
5. Web interface to the server
6. TIBCO Enterprise Message Service agent: The agent for TIBCO Enterprise Message Service is installed automatically. For configuration steps and more details on the agent, refer to *Agent for TIBCO Enterprise Message Service Guide.*
7. TIBCO Security Server agent: The agent for TIBCO Security Server is installed automatically. The agent is auto-registered with TIBCO Enterprise Administrator. There are no configuration steps. For more details on using the agent for TIBCO Security Server, refer to *Agent for TIBCO Security Server Guide.*
8. TIBCO Hawk Agent: This is an optional component that is installed only if you have opted for it.

A `samples` folder is available with a set of sample agents.

With 2.1 version of the release, the *`TIBCO_HOME`*`/tea/agents` folder is created with folders for TIBCO Enterprise Message Service and TIBCO Security Server agents.

## Installing in the Console Mode

After you prepare your system and the installation media, you can run the installer in the console mode.

### Procedure

1. Open the physical media or download the package.
2. Extract the contents of the package to a temporary directory.
3. Using a console window, navigate to the temporary directory.
4. Run the following:

   **Windows** `TIBCOUniversalInstaller -console`

   **UNIX** `TIBCOUniversalInstaller.bin -console`
5. Complete the installation by responding to the console window prompts.

## Installing in the Silent Mode

You can run the installer without user input by pointing the installer to a response file. A default configured response file exists.
In the silent mode, the installer does not prompt for inputs during installation but reads the inputs from a response file. By default, the installer uses the `TIBCOUniversalInstaller-`*`product_version`*`.silent` file, which is included in the directory that contains the universal installer.

You can customize the silent installer as follows:

- Make a backup copy of the file and edit the file itself. The name of the backup copy file depends on the variant of TIBCO Enterprise Administrator you are using. If you are using TIBCO Enterprise Administrator, use `TIBCOUniversalInstaller_tea_<version>.silent`. If you are using TIBCO Enterprise Administrator SDK, use `TIBCOUniversalInstaller_tea-sdk_<version>.silent`. You can then run the silent installer with or without the response file argument.
- Make a copy of the silent mode installer and name the copy. The name of the file depends on the variant of TIBCO Enterprise Administrator you are using. If you are using TIBCO Enterprise Administrator, use `TIBCOUniversalInstaller_tea_<version>.silent`. If you are using IBCO Enterprise Administrator SDK, use `TIBCOUniversalInstaller_tea-sdk_<`*`version`*`>.silent` file and name the copy. You can then run the silent installer, passing in your custom response file.

### Procedure

1. Open the physical media or download the package.
2. Extract the contents of the package to a temporary directory.
3. Using a console window, navigate to the temporary directory.
4. Make a copy of the `TIBCOUniversalInstaller_tea-sdk_<version>.silent` or `TIBCOUniversalInstaller_tea_<version>.silent` file and rename the file.
5. Using a text editor, open the copied file. You may need to update the install location, ENV_NAME, and features to install.
   a) Update the install location. The default location is: `<entry key="installationRoot">C:\tibco</entry>`.
   b) Update features to install. Set the features that you want to install to `true`.
   c) If you want to register the TIBCO Enterprise Administrator server as an NT service, include the following entry: `<entry key="teaWindowsServiceType"> manual</entry>`.

6. Run the silent installer with or without the optional response file.

   - **Windows**: `TIBCOUniversalInstaller.cmd -silent [-V responseFile="myfile.silent" ]`
   - **UNIX**: `TIBCOUniversalInstaller.bin -silent [-V responseFile='myfile.silent']`

## Postinstallation Steps for TIBCO Hawk Agent

The TIBCO Hawk agent is an optional component that you can install with TIBCO Enterprise Administrator.

A Hawk agent is an autonomous process that resides on each computer that monitors TIBCO applications on the computer.

The TIBCO Hawk agent operates autonomously and is active whenever the operating system it monitors is active. The Hawk agent uses a set of rules, called rulebases, to configure system management, status, and automation tasks. The Hawk agent monitors conditions on its local machine and send alerts over the network only when problems are detected.

TIBCO Hawk Agent can use one of the following products as the mode of transport:

1. TIBCO DataGrid (distributed as a part of Hawk installation)
2. TIBCO Rendezvous
3. TIBCO Enterprise Message Service

You must install one of the transport modes listed independent of the TIBCO Enterprise Administrator installation. You might have to follow some postinstallation steps depending upon the following:

1. You installed TIBCO Rendezvous or TIBCO Enterprise Message Service before installing TIBCO Hawk : In this case, follow the steps outlined in in the *Configuring TIBCO Hawk Components* chapter of the TIBCO Hawk Documentation.
2. The *TIBCO_HOME* selected for the transport mode(TIBCO Rendezvous or TIBCO Enterprise Message Service) is different from that of the Hawk*TIBCO_HOME*: In this case, follow the steps outlined in the section *Different TIBCO_HOME Locations for Various TIBCO Products* of the TIBCO Hawk Documentation.
3. If you want to use TIBCO DataGrid as the transport for the Hawk Agent bundled with TIBCO Enterprise Administrator, the *AS_HOME* should point to the standalone installation of TIBCO ActiveSpaces that is supported by Hawk 5.1.1.

# Installation Logs

The installer log file, `tibco_universal_installer.username_install.log`, is written to the `.TIBCO/install_timestamp` folder of the home directory. To change the location of the installer log file, specify the option `-V logFile="myLogFile"` when you run the installer .

The installer log file captures the following information:

- Installation environment details such as the user that invoked the installer, host name, *JAVA_HOME* in the environment, operating system details, and so on.
- List of assemblies installed.

# Configuring the TIBCO Enterprise Administrator Server

Assume that the location of the configuration folder selected during installation is *TIBCO_CONFIG_HOME*. The default configuration file `tea.conf` is available under `<TIBCO_CONFIG_HOME>\tibco\cfgmgmt\tea\conf`. To customize the server configuration, you can add additional properties to this file.

You can modify the following properties:

| Property Name | Description | Default Value |
|---|---|---|
| tea.http.port | The HTTP port on which the TIBCO Enterprise Administrator server listens to requests. | `8777` |
| tea.http.session.timeout | The HTTP Session Timeout for the TIBCO Enterprise Administrator server. | `1800 seconds` |
| tea.agents.ping-interval | The time interval in which the TIBCO Enterprise Administrator server pings each agent. | `15000 ms` |
| tea.auth.timeout | The timeout value for fetching the user configuration during login. | `60000 ms` |
| tea.shell.port | The port number to connect to the SSH server hosted by the TIBCO Enterprise Administrator server. | `2222` |
| tea.shell.timeout | The time for which the TIBCO Enterprise Administrator server waits for a response from the shell command. | `15000 ms` |
| tea.indexing.interval | The time taken for the elements to become available on the server after registration | `30000 ms` |
| tea.server.instance.name | When there are multiple instances of the server running, you can distinguish the instances by their instance name. The instance name appears under TIBCO Enterprise Administrator in the UI. | |
| tea.storage.remote.enabled | When set to true, the internal database is enabled for data sharing. | `true` |
| tea.storage.remote.tcpPort | Sets the port used by the internal database. | `9092` |
| tea.storage.remote.username | Use this property only if you plan to use TIBCO Enterprise Administrator from a CONFIG_HOME different from the existing one. | |

| Property Name | Description | Default Value |
|---|---|---|
| tea.storage.remote.password | This property is coupled with `tea.storage.remote.username`. Use this property only if you plan to use TIBCO Enterprise Administrator from a *CONFIG_HOME* different from the existing one. | |
| tea.ext.hawk.enabled | Set this property to `true` to enable Hawk server extension. | `false` |
| tea.dev.developer-mode | Set this property to `true` to start TIBCO Enterprise Administrator in the developer mode. | `false` |
| tea.jvminfo.enabled | Set this property to true view the JVM details on the server side. | `false` |

The format supported is HOCON. See http://github.com/typesafehub/config/blob/master/HOCON.md.

## SSL Configuration on the TIBCO Enterprise Administrator: An Overview

The TIBCO Enterprise Administrator supports both one-way (server side) and two-way (server side as well as client side) SSL authentication. You can configure SSL between the web browser and the TIBCO Enterprise Administrator as well as between the TIBCO Enterprise Administrator and the Agent.

- **One-way Authentication** - This is also known as server-side authentication. For this type of authentication the HttpClient residing in an application authenticates the HttpServer residing in another application. The HttpServer is not required to authenticate the HttpClient. On TIBCO Enterprise Administrator, this would mean:
  - The HttpClient residing on the TIBCO Enterprise Administrator server verifies the HttpServer residing on the Agent

    AND
  - The HttpClient residing on the Agent verifies the HttpServer residing on the TIBCO Enterprise Administrator server

So, the HttpServers residing on both the TIBCO Enterprise Administrator server and Agent simply trust each others' HttpClients.

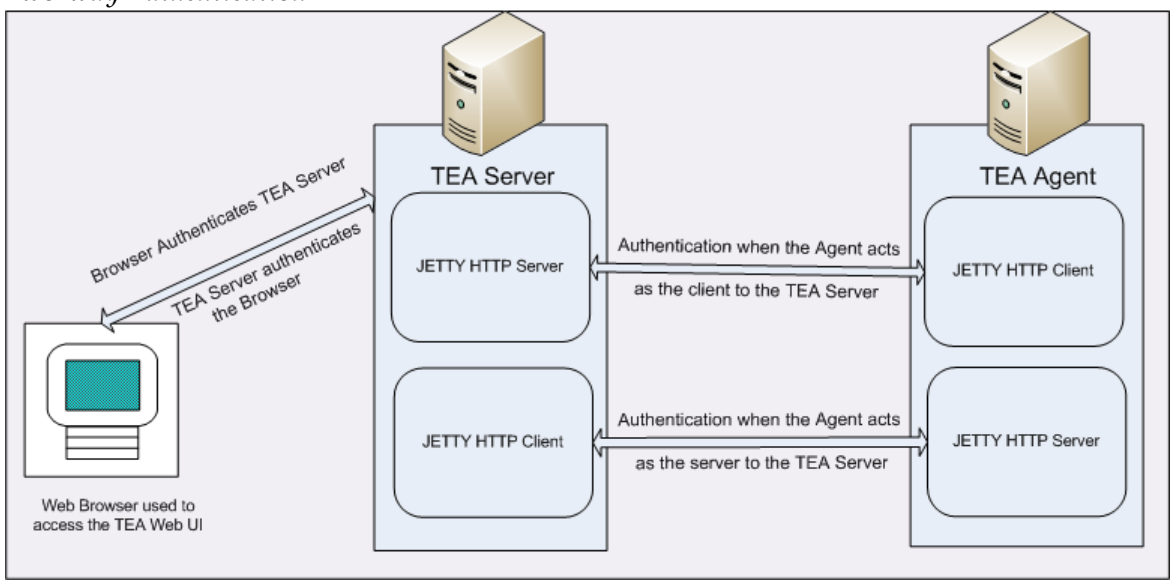
- **Two-way Authentication** - In addition to the server-side authentication used for the one-way authentication, the two-way authentication requires client-side authentication too. On TIBCO Enterprise Administrator, that would mean ALL of the following needs to happen:
  - The HttpClient residing on the TIBCO Enterprise Administrator server verifies the HttpServer residing on the Agent
  - The HttpClient residing on the Agent verifies the HttpServer residing on the TIBCO Enterprise Administrator server
  - The HttpServer residing on the TIBCO Enterprise Administrator server verifies the HttpClient residing on the Agent
  - The HttpServer residing on the Agent verifies the HttpClient residing on the TIBCO Enterprise Administrator server

Earlier versions of TIBCO Enterprise Administrator supported only one-way authentication. TIBCO Enterprise Administrator 1.3.0 and above supports two-way authentication. However, you always have the option to implement one-way authentication alone too.

In TIBCO Enterprise Administrator, the web browser (which you use to run the TIBCO Enterprise Administrator web UI) is a client to the TIBCO Enterprise Administrator server. The TIBCO Enterprise Administrator server on the other hand, acts as a client to the Agent when it makes a request to the Agent, but acts as a server to the Agent when the Agent requests some information from it. Similarly the Agent acts as a server to the TIBCO Enterprise Administrator server when fulfilling a request from the TIBCO Enterprise Administrator server but acts as a client to the TIBCO Enterprise Administrator server when making a request to the TIBCO Enterprise Administrator server(such as when getting itself registered with the TIBCO Enterprise Administrator server).

The following diagram shows a very high level overview of authentication in a two-way authentication setup:

*Two-way Authentication*




## Configuring SSL: One-Way Authentication

To configure a one-way SSL authentication, you must set some SSL-related properties in the `tea.conf` file as well as on the Agent.

### Procedure

1. Open *<TIBCO_CONFIG_HOME>*`\tibco\cfgmgmt\tea\conf\tea.conf`.
2. Add the properties listed in the section, SSL Properties in the `tea.conf` file.

   The following is an example of the `tea.conf` file with SSL settings:

```
tea.http.keystore = "/Users/<username>/tea/keystore/httpserversslkeys.jceks"
tea.http.truststore = "/Users/<username>/tea/keystore/httpserverssltrusts.jceks"
tea.http.keystore-password = "password"
tea.http.truststore-password = "password"
tea.http.key-manager-password = "password"
tea.http.cert-alias = "httpserver"
tea.http.want.client.auth = false
tea.http.need.client.auth = false
```

The TIBCO Enterprise Administrator server supports the keystore formats supported by Java. Therefore, keystore formats such as, `jks`, `jceks`, `pkcs12` are supported by the TIBCO Enterprise Administrator server. For a detailed list of supported keystore formats, refer to the *KeyStore Types* documentation on the Oracle Website.

3. Set the same properties on the Agent. Refer to the section, "Setting SSL Properties on the Agent", in the *TIBCO Enterprise Administrator Developer's Guide*.

## Configuring SSL: Two-Way Authentication

Two-way SSL authentication requires you to configure both server-side authentication and client-side authentication.
To set up this two-way authentication, you need to perform the following steps. You can perform these steps in one of the two ways - either using the keytool (to be run from your `<JAVA_HOME>/bin` directory) or by running the commands specified on the OpenSSL documentation website, http://wiki.openssl.org/index.php/Command_Line_Utilities.

### Procedure

1. Follow the steps outlined in Configuring SSL: One-Way Authentication.
2. Generate the key store and private key for the HttpServer on the TIBCO Enterprise Administrator server and the HttpServer on the Agent.
3. Generate a self-signed certificate or obtain a CA-signed certificate for the HttpServer on the TIBCO Enterprise Administrator server and the HttpServer on the Agent.
4. Generate the key store and private key for the HttpClient on the TIBCO Enterprise Administrator server and the HttpClient on the Agent.
5. Generate a self-signed certificate or obtain a CA-signed certificate for the HttpClient on the TIBCO Enterprise Administrator server and the HttpClient on the Agent.
6. Import the Agent HttpServer's certificate into the trust store used by TIBCO Enterprise Administrator server's HttpClient.
7. Import the TIBCO Enterprise Administrator server's HttpServer's certificate into the Agent's HttpClients' trust store.
8. For the web browser (from where you will be accessing the TIBCO Enterprise Administrator UI): Generate a PKCS #12 format certificate which will include a private key for the browser and a public key and the browser's certificate.
9. Import the certificate from the above step into the web browser's trust store. Refer to the browser's documentation for details on importing the certificate into the browser.

### Result

Once the SSL configuration has been set up and is working, the URL to access the TIBCO Enterprise Administrator server from the web UI will change from http://localhost:8777 to https://localhost:8777.

# SSL Properties

When configuring SSL on the TIBCO Enterprise Administrator, you need to set some properties on both the TIBCO Enterprise Administrator server as well as the Agent.

Setting the HttpClient properties on both the Agent and the TIBCO Enterprise Administrator server is mandatory **only** if you want to set up a two-way SSL configuration. You do not need to set the HttpClient properties if you want to set up a one-way SSL configuration or do not want to set up SSL at all. If you do not set the HttpClient properties on the Agent and the TIBCO Enterprise Administrator server, the HttpClients residing on both of them will be configured to "Trust All".

To enable SSL on the TIBCO Enterprise Administrator server, set these properties for the HttpServer and HttpClient residing on the TIBCO Enterprise Administrator server:

*TIBCO Enterprise Administrator Server Properties*

| Property | Description |
|---|---|
| **Properties for the HttpServer on the TIBCO Enterprise Administrator server** | |
| tea.http.keystore | The file name or URL of the key store location<br>For example: `tea.http.keystore = "/Users/<username>/tea/keystore/httpserversslkeys.jceks"` |
| tea.http.keystore-password | Password for the key store residing on the TIBCO Enterprise Administrator server. This is the password that was set when the key store was created<br>For example:<br>`tea.http.keystore-password = "MyPassword"` |
| tea.http.cert-alias | Alias for the SSL certificate. The certificate can be identified by this alias in case there are multiple certificates in the trust store<br>For example:<br>`tea.http.cert-alias = "httpserver"` |
| tea.http.key-manager-password | The password for the specific key within the key store. This is the password that was set when the key pair was created<br>For example:<br>`tea.http.key-manager-password = "password"` |
| tea.http.truststore | The file name or URL of the trust store location<br>For example:<br>`tea.http.truststore = "/Users/<username>/tea/keystore/httpserverssltrusts.jceks"` |
| tea.http.truststore-password | The password for the trust store<br>For example:<br>`tea.http.truststore-password = "password"` |
| tea.http.want.client.auth | See section Guidelines to set the tea.http.want.client.auth and tea.http.need.client.auth Parameters below. This property is used for mutual authentication<br>For example:<br>`tea.http.want.client.auth = true` |
| tea.http.need.client.auth | See section Guidelines to set the tea.http.want.client.auth and tea.http.need.client.auth Parameters below. This property is used for mutual authentication<br>For example:<br>`tea.http.need.client.auth = true` |

| Property | Description |
|---|---|
| tea.http.exclude.protocols | The property to list the protocols to be excluded. To exclude multiple protocols, use comma as a delimiter.<br>For example, `tea.http.exclude.protocols="SSLv3,TLS1"`<br>If the property is *not* mentioned, the SSLV3 protocol is excluded. If TIBCO Enterprise Administrator server must support all protocols including SSLV3, set the property to be empty.<br>For example, `tea.http.exclude.protocols=""`<br>When connecting using HTTPS, some versions of the popular browsers may be configured to use SSLv3 as the protocol. If you have problems accessing secured TIBCO Enterprise Administrator server (by default the SSLv3 is disabled) using the browser, follow the browser's user guide to configure that browser to excludeSSLv3 protocol. |
| **Properties for the HttpClient on the TIBCO Enterprise Administrator server**<br>Only required if you want to set up a two-way SSL configuration | |
| tea.http.client.keystore | The file name or URL of the key store location<br>For example:<br>`tea.http.client.keystore = "/Users/<username>/tea/keystore/httpclientsslkeys.jceks"` |
| tea.http.client.keystore-password | The password for the key store residing on the client (Agent)<br>For example:<br>`tea.http.client.keystore-password = "password"` |
| tea.http.client.cert-alias | Alias for the SSL certificate. The certificate can be identified by this alias in case there are multiple certificates in the trust store<br>For example:<br>`tea.http.client.cert-alias = "httpclient"` |
| tea.http.client.key-manager-password | The password for the specific key within the key store<br>For example:<br>`tea.http.client.key-manager-password = "password"` |
| tea.http.client.truststore | The file name or URL of the trust store location<br>For example:<br>`tea.http.client.truststore = "/Users/<username>/tea/keystore/httpclientssltrusts.jceks"` |
| tea.http.client.truststore-password | The password for the trust store<br>For example:<br>`tea.http.client.truststore-password = "password"` |

| Property | Description |
|---|---|
| tea.http.client.exclude.protocols | The property to list the protocols to be excluded. To exclude multiple protocols, use comma as a delimiter.<br>For example, `tea.http.exclude.protocols="SSLv3,TLS1"`<br>If the property is *not* mentioned, the SSLV3 protocol is excluded. If TIBCO Enterprise Administrator server must support all protocols including SSLV3, set the property to be empty.<br>For example, `tea.http.exclude.protocols=""`<br>When connecting using HTTPS, some versions of the popular browsers may be configured to use SSLv3 as the protocol. If you have problems accessing secured TIBCO Enterprise Administrator server (by default the SSLv3 is disabled) using the browser, follow the browser's user guide to configure that browser to excludeSSLv3 protocol. |

***Agent Properties***

To enable SSL on the Agent, set the following properties for the HttpServer and HttpClient residing on the Agent:

| Property | Description |
|---|---|
| **Properties for the HttpServer on the Agent** | |
| tea.agent.http.keystore | The file name or URL of the key store location<br>For example: `tea.agent.http.keystore = "/Users/<username>/tea/keystore/httpserversslkeys.jceks"` |
| tea.agent.http.keystore.password | Password for the key store residing on the Agent. This is the password that was set when the key store was created<br>For example:<br>`tea.agent.http.keystore.password = "MyPassword"` |
| tea.agent.http.cert.alias | Alias for the SSL certificate. The certificate can be identified by this alias in case there are multiple certificates in the trust store<br>For example:<br>`tea.agent.http.cert.alias = "httpserver"` |
| tea.agent.http.keymanager.password | The password for the specific key within the key store. This is the password that was set when the key pair was created<br>For example:<br>`tea.agent.http.keymanager.password = "password"` |

| Property | Description |
|---|---|
| tea.agent.http.truststore | The file name or URL of the trust store location<br>For example:<br>`tea.agent.http.truststore = "/Users/<username>/tea/keystore/httpserverssltrusts.jceks"` |
| tea.agent.http.truststore.password | The password for the trust store<br>For example:<br>`tea.agent.http.truststore.password = "password"` |
| tea.agent.http.want.client.auth | See section Guidelines to set the tea.http.want.client.auth and tea.http.need.client.auth Parameters below. This property is used for mutual authentication<br>For example:<br>`tea.agent.http.want.client.auth = true` |
| tea.agent.http.need.client.auth | See section Guidelines to set the tea.http.want.client.auth and tea.http.need.client.auth Parameters below. This property is used for mutual authentication<br>For example:<br>`tea.agent.http.need.client.auth = true` |
| tea.agent.http.exclude.protocols | The property to list the protocols to be excluded. To exclude multiple protocols, use comma as a delimiter.<br>For example, `tea.http.exclude.protocols="SSLv3,TLS1"`<br>If the property is *not* set either using system properties or using Agent Server API, the SSLV3 protocol is excluded. If TIBCO Enterprise Administrator Agent must support all protocols including SSLV3, set the property to be empty.<br>For example, `tea.http.exclude.protocols=""`<br>When connecting using HTTPS, some versions of the popular browsers may be configured to use SSLv3 as the protocol. If you have problems accessing secured TIBCO Enterprise Administrator server (by default the SSLv3 is disabled) using the browser, follow the browser's user guide to configure that browser to excludeSSLv3 protocol. |
| **Properties for the HttpClient on the Agent**<br>Only required if you want to set up a two-way SSL configuration | |
| tea.agent.http.client.keystore | The file name or URL of the key store location<br>For example:<br>`tea.agent.http.client.keystore = "/Users/<username>/tea/keystore/httpclientsslkeys.jceks"` |

| Property | Description |
|---|---|
| tea.agent.http.client.keystore.password | The password for the key store residing on the client (Agent)<br>For example:<br>`tea.agent.http.client.keystore.password = "password"` |
| tea.agent.http.client.cert.alias | Alias for the SSL certificate. The certificate can be identified by this alias in case there are multiple certificates in the trust store<br>For example:<br>`tea.agent.http.client.cert.alias = "httpclient"` |
| tea.agent.http.client.keymanager.password | The password for the specific key within the key store<br>For example:<br>`tea.agent.http.client.keymanager.password = "password"` |
| tea.agent.http.client.truststore | The file name or URL of the trust store location<br>For example:<br>`tea.agent.http.client.truststore = "/Users/<username>/tea/keystore/httpclientssltrusts.jceks"` |
| tea.agent.http.client.truststore.password | The password for the trust store<br>For example:<br>`tea.agent.http.client.truststore.password = "password"` |
| tea.agent.http.client.exclude.protocols | The property to list the protocols to be excluded. To exclude multiple protocols, use comma as a delimiter.<br>For example, `tea.http.exclude.protocols="SSLv3,TLS1"`<br>If the property is *not* set either using system properties or using Agent Server API, the SSLV3 protocol is excluded. If TIBCO Enterprise Administrator Agent must support all protocols including SSLV3, set the property to be empty.<br>For example, `tea.http.exclude.protocols=""`<br>When connecting using HTTPS, some versions of the popular browsers may be configured to use SSLv3 as the protocol. If you have problems accessing secured TIBCO Enterprise Administrator server (by default the SSLv3 is disabled) using the browser, follow the browser's user guide to configure that browser to excludeSSLv3 protocol. |

### Guidelines to set the tea.http.want.client.auth and tea.http.need.client.auth Parameters

Here are some guidelines for setting these parameters depending on the scenario you want to implement:

| For this type of authentication... | setting the parameters in this combination... | will result in... |
|---|---|---|
| Certification-based two-way authentication | http.want.client.auth = true<br>http.need.client.auth = false | The TEA server asks the client (web browser or Agent) to provide its client certificate while handshaking. But the client chooses not to provide authentication information about itself, but the authentication process will continue.<br>So that would mean that the client certification is optional which in turn means that no certificate needs to be generated on the client.<br>**End Result**<br>The authentication process is successful. |
| | http.want.client.auth = false<br>http.need.client.auth = true | The TEA server asks the client (web browser or Agent) to provide its client certificate while handshaking, but the client chooses not to provide authentication information about itself, the authentication process will stop.<br>So that would mean that the client certification is required which in turn means that a keypair and certificate must be generated on the client (Agent).<br>**End Result**<br>The authentication process fails |
| | http.want.client.auth = true<br>http.need.client.auth = true | Same as the above case where the client certification is required and a keypair and certificate must be generated on the client (Agent).<br>**End Result**<br>The authentication process fails |
| Certification-based one-way authentication | http.want.client.auth = false<br>http.need.client.auth = false | Both of the parameters set to 'false' which means that it is a One-way Authentication, where only the client (web browser or Agent) will verify the TEA server but the TEA server trusts all the clients without verification.<br>No need to generate any certificates at all.<br>**End Result**<br>The authentication process is successful, as long as the user name and password provided by the agent are both correct. |

## Setting SSL Properties on the Agent

To enable SSL, you must set the SSL system properties on both the TIBCO Enterprise Administrator server and the Agent.

Refer to the SSL Properties section for details on the system properties to be set.

### Procedure

1. On the Agent, you can set the SSL system properties in **one** of the following ways:

   - Set the properties using the API.

     For example,

     ```
     server.setKeystorePath(
     “/tea/keystore/httpserversslkeys.jceks”
     server.setKeyStorePath("/tea/keystore/httpserversslkeys.jceks");
     server.setKeyStorePassword("password");
     server.setCertAlias("httpserver");
     server.setTrustStorePath("/tea/keystore/httpserverssltrusts.jceks");
     server.setTrustStorePassword("password");
     server.setKeyManagerPassword("password");
     server.setWantClientAuth(true);
     server.setNeedClientAuth(true);

     server.setHttpClientKeyStorePath("/tea/keystore/httpclientsslkeys.jceks");
     server.setHttpClientKeyStorePassword("password");
     server.setHttpClientCertAlias("httpclient");
     server.setHttpClientTrustStorePath("/tea/keystore/
     httpclientssltrusts.jceks");
     server.setHttpClientTrustStorePassword("password");
     server.setHttpClientKeyManagerPassword("password");
     ```

   - Create an SSLContext and inject it into the TIBCO Enterprise Administrator server using the Agent API.

     To do so:

     1. Create an SSLContext object. Follow the JDK documentation on the Oracle web site for instructions on how to do so.
     2. Use the SSLContext API to set the configuration properties into the SSLContext instance. Follow the JDK documentation on the Oracle web site for instructions on how to do so.
     3. Inject the SSLContext instance into the TEA Agent's HttpServer and HttpClient using one of the following APIs:

        ```
        public TeaAgentServer(final String name, final String version, final
        String agentinfo, final int port, final String contextPath,
        final Boolean enableMetrics, final SSLContext sslContextForHttpServer,
        final SSLContext sslContextForHttpClient)
        ```

        or

        ```
        public TeaAgentServer(final String name, final String version, final
        String agentinfo, final String hostname, final int port,
        final String contextPath, final Boolean enableMetrics, final SSLContext
        sslContextForHttpServer, final SSLContext sslContextForHttpClient)
        ```

        If you choose not to specify the hostname parameter as shown in the first interface above, a default value of localhost will be used for the hostname.

        An example of using the first API above:

        ```
        final TeaAgentServer server = new
        TeaAgentServer("SSLTestAgent","1.1","Agent for SSL test",port,"/
        ssltestagent",true,
        sslContextForServer, sslContextForClient);
        ```

- Set the properties from the command line using these System.properties when running the Agent.

  For example,

```
-Dtea.agent.http.keystore="/Users/<username>/tea/keystore/
httpserversslkeys.jceks"
-Dtea.agent.http.truststore="/Users/<username>/tea/keystore/
httpserverssltrusts.jceks"
-Dtea.agent.http.keystore.password="password"
-Dtea.agent.http.truststore.password="password"
-Dtea.agent.http.keymanager.password="password"
-Dtea.agent.http.cert-alias="httpserver"
-Dtea.agent.http.want.client.auth=true
-Dtea.agent.http.need.client.auth=true
-Dtea.agent.http.client.keystore="/Users/<username>/tea/keystore/
httpclientsslkeys.jceks"
-Dtea.agent.http.client.truststore="/Users/<username>/tea/keystore/
httpclientssltrusts.jceks"
-Dtea.agent.http.client.keystore.password="password"
-Dtea.agent.http.client.truststore.password="password"
-Dtea.agent.http.client.keymanager.password="password"
-Dtea.agent.http.client.cert-alias="httpclient"
```

2. Start the Agent. If you did not set the system properties using the API or create and inject an SSLContext, then make sure to start the Agent in SSL mode by setting the properties through the command line as shown in the example in the last bullet item above.

## Configuring Properties to Enable Hawk Integration

To integrate TIBCO Enterprise Administrator with Hawk, some properties must be set in the *<TIBCO_HOME>*\tea\<version>\bin\tea.tra file.

Based on the transport type selected, the following properties need to be modified to integrate TIBCO Enterprise Administrator with Hawk:

```
# Variables for TEA and HAWK Integration
# IMPORTANT:: Product HOME(s) should include version folder

# HAWK TIBCO home
#tibco.env.HAWK_HOME=[[TIBCO_HAWK_HOME_ESC]]

# ActiveSpaces TIBCO HOME
#tibco.env.AS_HOME=[[TIBCO_AS_HOME_ESC]]

# Enterprise Message Service TIBCO HOME
#tibco.env.EMS_HOME=[[TIBCO_EMS_HOME_ESC]]

# Rendezvous TIBCO HOME
#tibco.env.RV_HOME=[[TIBCO_RV_HOME_ESC]]}
```

Ensure that the tibco.env.HAWK_HOME specified in the *<TIBCO_HOME>*\tea\<version>\bin\tea.tra file points to the *HAWK_HOME* location. By default, if no transport type is specified, the default transport type is set to TIBCO ActiveSpaces. Depending on the transport type used, ensure that you specify one of the following:

| Transport Type | Property in The tea.tra File | Points to |
|---|---|---|
| TIBCO ActiveSpaces | tibco.env.AS_HOME | TIBCO_ACTIVESPACES_HOME |
| TIBCO Enterprise Message Service | tibco.env.EMS_HOME | TIBCO_EMS_HOME |
| TIBCO Rendezvous | tibco.env.RV_HOME | TIBCO_RV_HOME |

For example, if the transport type is TIBCO Enterprise Message Service, ensure that the`tibco.env.EMS_HOME` points to `TIBCO_EMS_HOME`.

If TIBCO Enterprise Administrator is installed in the same *TIBCO_HOME* as the transport types used, the `tibo.env.<transport_type>.home` variable is automatically set to point to the appropriate `TIBCO_<transport_type>_HOME`.

# Setting Up Data Sharing on the Server

If you want to, you can set some properties to enable the Data Sharing API on the TIBCO Enterprise Administrator server. These properties are set in the *TIBCO_HOME*\tibco\cfgmgmt\tea\conf\tea.conf file.

### Procedure

1. Modify the following property to enable TIBCO Enterprise Administrator internal database for data sharing:
   ```
   tea.storage.remote.enabled=true
   ```
   By default, the property is set to `true`.
2. Add the port used by the internal database.
   ```
   # Port used by TEA internal Database
   tea.storage.remote.tcpPort=9092
   ```
   
   If the agents accessing the server are not on the same machine as the TIBCO Enterprise Administrator server, the configuration property `tea.http.host` should be set to the IP address of the machine running the TIBCO Enterprise Administrator server.
3. Add the username and password to connect to the internal database. By default, these fields are empty.
   ```
   # Please do not uncomment username and password properties if you
    plan to use TEA in an existing TEA_CONFIG_HOME
   # If you plan to use TEA in a fresh CONFIG_HOME (fresh database),
   you can uncomment username and password properties and set the
   appropriate values

   #tea.storage.remote.username=
   #tea.storage.remote.password=
   ```
   There is currently no support in TIBCO Enterprise Administrator to change the username and password for the DDBB, so an external utility should be used to manage DDBB.

# Upgrade

The steps to upgrade are similar to the steps listed in the Installation section of the guide. You can install 2.2 in the same *TIBCO_HOME* or select a different *TIBCO_HOME*. You can optionally choose a configuration folder to store the configuration related data. Assuming that *TIBCO_CONFIG_HOME* is used to represent the configuration folder selected, the default location of the configuration related data is *TIBCO_CONFIG_HOME*\tibco\cfgmgmt\tea.

When you install TIBCO Enterprise Administrator in an existing *TIBCO_HOME*, the universal installer does not prompt for a *TIBCO_CONFIG_HOME*. This is because the universal installer associates *TIBCO_CONFIG_HOME* with a *TIBCO_HOME*.

The *TIBCO_CONFIG_HOME* location can be different from the one you are currently using. If so, to avoid re-registering agents, start the server with the existing `data`, `conf`, and `log` locations. The following shows the different ways of starting the server based on the location of the configuration folder:

| Scenario | How to Start the TIBCO Enterprise Administrator server |
|---|---|
| To start the TIBCO Enterprise Administrator server with a different `data` folder. | **Unix**<br>**`./tea -data <location of the data folder>`**<br>**Windows**<br>**`tea.exe -data <location of the data folder>`** |
| To start the TIBCO Enterprise Administrator server with a different `conf` folder. | **Unix**<br>**`./tea -conf <location of the conf folder>`**<br>**Windows**<br>**`tea.exe -conf <location of the conf folder>`** |
| To start the TIBCO Enterprise Administrator server with a different `logs` folder. | **Unix**<br>**`./tea -logs <location of the logs folder>`**<br>**Windows**<br>**`tea.exe -logs <location of the logs folder>`** |

As an alternative, you can pass these parameters from the command line to override the ones set in the `tea.tra` file.

# Backward Compatibility

This section discusses scenarios where different server versions need to coexist with different agent library versions, scenarios where existing agents get upgraded, or two different versions of agents are managing two different versions of the product.

### Coexistence of Server Versions and Agent Library Versions

| Server → / Agent Library ↓ | 1.0.0 | 1.0.0 Hotfix | 1.0.x | 1.1.0 | 1.1.x | 1.2.0 | 1.3.0 | 2.0.0 | 2.1.0 | 2.2.0 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1.0.0 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| 1.0.0 Hotfix | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| 1.0.x | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| 1.1.0 | No | No | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| 1.1.x | No | No | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| 1.2.0 | No | No | No | No | No | Yes | Yes | Yes | Yes | Yes |
| 1.3.0 | No | No | No | No | No | No | Yes | Yes | Yes | Yes |
| 2.0.0 | No | No | No | No | No | No | No | Yes | Yes | Yes |
| 2.1.0 | No | No | No | No | No | No | No | No | Yes | Yes |
| 2.2.0 | No | No | No | No | No | No | No | No | No | Yes |

Agents built with a higher version of the library cannot be registered with a lower version of the server.

# Uninstallation

Uninstall TIBCO products with TIBCO Universal Installer. The installer runs on multiple platforms. You can run the installer in the GUI mode, console mode, or silent mode.

## Uninstalling in the GUI Mode

This section describes how to uninstall this product in the GUI mode and the Console mode.

### Procedure

1. Shut down all running TIBCO applications.
2. Navigate to `<TIBCO_HOME>\tools\universal_installer` and run TIBCOUniversalInstaller.
3. In the TIBCO Installation Manager pane:
   a) Select the **Uninstall Products From Selected TIBCO Home Location** radio button.
   b) Select the *TIBCO_HOME* location from the **TIBCO Home Location** drop-down list.
   c) In the Welcome window, click **Next**.
4. Select an uninstallation option. The wizard provides two uninstallation options:
   a) **Custom Uninstall**: You can select the products to be removed.
   b) **Typical Uninstall**: The universal uninstaller removes all the products in this *TIBCO_HOME*.
5. Click **Next**. If you selected the **Custom Uninstall (Select The Products To Be Removed)** radio button, select the check boxes for products to uninstall, and then click **Uninstall.**
6. Review the Pre-Uninstall Summary and click the **Uninstall** button to start the uninstallation process.
7. Review the Post-Uninstall Summary and click the **Finish** button to exit the uninstall wizard.

After the uninstallation, you have to manually delete some of the folders related to TIBCO Enterprise Administrator. They are safe to delete provided they are not related to *TIBCO_CONFIG_HOME*.

## Uninstalling in the Console Mode

You can uninstall this product in the console mode.

### Procedure

1. Using a command window, navigate to the `<TIBCO_HOME>\tools\universal_installer` directory.
2. Type the following command at the command prompt: `TIBCOUniversalInstaller.exe -console`
3. Complete the uninstallation by responding to the console window prompts.

After the uninstallation, you have to manually delete some of the folders related to TIBCO Enterprise Administrator. They are safe to delete provided they are not related to *TIBCO_CONFIG_HOME*.