## Contents

### About This Guide
- Overview .................................................. 9
- Document List ........................................... 9
- Document Conventions ................................ 10
- Contact Information ...................................... 11

### Chapter 1. Installing Tripwire Enterprise Console
- Installation Overview .................................. 13
- Configuring the Tripwire Enterprise Database .... 14
  - Database Requirements .............................. 14
  - Database Installation & Configuration .......... 14
- New Installations of Tripwire Enterprise Console 25
  - Step 1: Verify Hardware, Software, and Network Requirements 25
  - Step 2: Install Java Components .................. 26
  - Step 3: Install Tripwire Enterprise Console ..... 27
  - Tripwire Enterprise Console Services and Ports 30
- Upgrading Tripwire Enterprise Console .......... 33
  - Step 1: Verify Hardware and Software Requirements 33
  - Step 2. Back Up Data and Configuration Files 33
  - Step 3. Upgrade Tripwire Enterprise Console 34
  - Step 4. Restart Tripwire Enterprise Agents ...... 35
  - After Upgrading ...................................... 35
- Uninstalling Tripwire Enterprise Console ...... 37

### Chapter 2. Installing Tripwire Enterprise Agent
- Installation Requirements for Tripwire Enterprise Agent 40
- About Interactive and Silent Installations ........ 40
Chapter 3. Installing Tripwire Axon Agent ......................................................... 80

Getting Started with Tripwire Axon Agent ......................................................... 81
  Supported Platforms ......................................................................................... 81
  Required Ports and Protocols ........................................................................ 82
Installing Axon Agent ........................................................................................... 83
  Step 1. Configuring the Axon Bridge ................................................................. 83
  Step 2. (Optional) Configuring a DNS SRV Record ........................................ 85
  Step 3. Installing Axon Agent Software ......................................................... 86
  Step 4. Configuring Axon Agent ...................................................................... 90
  Silent Installation of Axon Agent .................................................................... 94
Using Tag Files to Assign Tags to New Axon Agents ........................................ 96
Upgrading Axon Agent ....................................................................................... 98
Uninstalling Axon Agent ..................................................................................... 101
Other Axon Agent Procedures ........................................................................... 102
  Determining an Axon Agent's Version ......................................................... 102
<table>
<thead>
<tr>
<th>Chapter 4. Post-Installation Configuration</th>
<th>113</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Tripwire Enterprise Inside a Network Address Translation (NAT) Environment</td>
<td>114</td>
</tr>
<tr>
<td>Configuring a Tripwire Enterprise Agent for Use on a Multi-NIC System</td>
<td>116</td>
</tr>
<tr>
<td>Configuring a Tripwire Enterprise Proxy for Agent Communication</td>
<td>117</td>
</tr>
<tr>
<td>Step 1. Configuring Your Tripwire Enterprise Server</td>
<td>117</td>
</tr>
<tr>
<td>Step 2. Installing and Configuring the Tripwire Enterprise Proxy</td>
<td>118</td>
</tr>
<tr>
<td>Step 3. Configuring TE Agents for Communication with the Proxy</td>
<td>119</td>
</tr>
<tr>
<td>Step 4. Configuring the Firewall</td>
<td>120</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 5. Maintenance Procedures</th>
<th>121</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance of Tripwire Enterprise</td>
<td>122</td>
</tr>
<tr>
<td>Backing Up and Restoring Tripwire Enterprise</td>
<td>123</td>
</tr>
<tr>
<td>Backing Up Tripwire Enterprise Data and Configuration Files</td>
<td>123</td>
</tr>
<tr>
<td>Restoring Tripwire Enterprise Data and Configuration Files</td>
<td>125</td>
</tr>
<tr>
<td>Updating Java for Tripwire Enterprise Console</td>
<td>127</td>
</tr>
<tr>
<td>Changing the Console Used to Manage an Agent</td>
<td>129</td>
</tr>
<tr>
<td>Changing the TE Console Used to Manage a TE Agent</td>
<td>129</td>
</tr>
<tr>
<td>Changing the TE Console Used to Manage an Axon Agent</td>
<td>130</td>
</tr>
<tr>
<td>Changing the Services and Database Passphrases</td>
<td>131</td>
</tr>
<tr>
<td>Changing the Tripwire Enterprise Services Passphrase</td>
<td>131</td>
</tr>
<tr>
<td>Changing the Tripwire Enterprise Database Passphrase</td>
<td>132</td>
</tr>
<tr>
<td>Managing Tripwire Enterprise Services</td>
<td>133</td>
</tr>
</tbody>
</table>
About This Guide

Overview

The Tripwire Enterprise Installation & Maintenance Guide includes the following sections:

- **Chapter 1: Installing Tripwire Enterprise Console (on page 12)** describes the process for installing Tripwire Enterprise Console software.
- **Chapter 2: Installing Tripwire Enterprise Agent (on page 39)** describes the process for installing Tripwire Enterprise Agent (TE Agent) software.
- **Chapter 3: Installing Tripwire Axon Agent (on page 80)** describes the process for installing Tripwire Axon Agent (Axon Agent) software.
- **Chapter 4: Post-Installation Configuration (on page 113)** includes optional post-installation configuration procedures.
- **Chapter 5: Maintenance Procedures (on page 121)** includes procedures used to maintain your Tripwire Enterprise implementation.

Document List

The Tripwire Enterprise Installation & Maintenance Guide provides installation and upgrade instructions for Tripwire Enterprise software. In addition, this guide includes procedures for the maintenance of your Tripwire Enterprise software and database.

The Tripwire Enterprise User Guide provides a detailed overview of Tripwire Enterprise functionality, along with related concepts and procedures.

The Tripwire Enterprise Reference Guide contains supplemental information for the operation of Tripwire Enterprise software and associated applications.

PDF versions of these documents are available:

- on the Downloads page of the Tripwire Customer Center (https://tripwireinc.force.com/customers)
- in the docs directory of the Tripwire Enterprise installation DVD
- in the TE Console download archive

In addition, online help may be accessed from the Tripwire Enterprise interface. The online help includes the content of all documents cited above.
## Document Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bolding</strong></td>
<td>Indicates:</td>
</tr>
<tr>
<td></td>
<td>- The labels of buttons, menus, fields, drop-downs, and check boxes.</td>
</tr>
<tr>
<td></td>
<td>- Options selected from a drop-down list or menu.</td>
</tr>
<tr>
<td></td>
<td>- Keystrokes and menu paths.</td>
</tr>
<tr>
<td></td>
<td>- Introductory sentences for procedures.</td>
</tr>
<tr>
<td></td>
<td>- The first reference of a term.</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>- In the Monitor dialog, select the <strong>Activate</strong> check box.</td>
</tr>
<tr>
<td></td>
<td>- Press <strong>CTRL+DELETE</strong>.</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Indicates cross references to sections and chapters in this book, as well as the titles of other books.</td>
</tr>
<tr>
<td></td>
<td>Example: &quot;For more information, see <em>Creating a Node.</em>&quot;</td>
</tr>
<tr>
<td><strong>Sans Serif</strong></td>
<td>Indicates:</td>
</tr>
<tr>
<td></td>
<td>- URLs and e-mail addresses</td>
</tr>
<tr>
<td></td>
<td>- Directory paths and file names</td>
</tr>
<tr>
<td></td>
<td>- Command-line entries</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>- <a href="http://www.tripwire.com">www.tripwire.com</a></td>
</tr>
<tr>
<td></td>
<td>- C:\Program Files\</td>
</tr>
<tr>
<td><strong>Brackets</strong></td>
<td>Indicates a set of possible user-entered options; individual options are separated by the pipe (</td>
</tr>
<tr>
<td></td>
<td>Example: [ 1</td>
</tr>
<tr>
<td><strong>Angle brackets</strong></td>
<td>Indicates placeholders for user-entered values.</td>
</tr>
<tr>
<td></td>
<td>Example: &lt;a_variable&gt;</td>
</tr>
</tbody>
</table>
Contact Information

Tripwire, Inc.

101 SW Main St., Ste. 1500
Portland, OR 97204
Web site: http://www.tripwire.com
Main: 503.276.7500
Fax: 503.223.0182
US Toll-free: 1.800.TRIPWIRE (1.800.874.7947)

Tripwire Sales

Domestic: sales@tripwire.com
Government: govt@tripwire.com
EMEA: emeasales@tripwire.com
APAC: apacsales@tripwire.com
Japan: japansales@tripwire.com

Tripwire Technical Support

Online support: https://www.tripwire.com/customers
Support policies: http://www.tripwire.com/customers/support-policy.cfm
Contact: https://secure.tripwire.com/customers/contact-support.cfm

Tripwire Professional Services

Tripwire Professional Services provides a wide range of services, including Tripwire Quickstarts, Turnkey Implementations, Change Auditing, and Process Improvement. For more information, please visit http://www.tripwire.com/services or contact your Tripwire sales representative.

Tripwire Educational Services

Tripwire Educational Services provides hands-on technical training for the installation, configuration, and maintenance of your Tripwire software. All courses are taught by Tripwire Certified Instructors. For more information, please contact your Tripwire sales representative or visit http://www.tripwire.com/services/training.
Chapter 1. Installing Tripwire Enterprise Console
**Installation Overview**

To install Tripwire Enterprise Console (TE Console), you can either perform a **new installation** or an **upgrade** from a previous version of the software. Use the chart below to identify the appropriate steps in the installation process.

Note the following terms related to TE Console installations:

- A **Tripwire Enterprise Server** is the host machine on which **Tripwire Enterprise Console** software is installed.
- The **TE database** or **backend database** stores the data generated by TE Console.
- TE Console and the TE database are normally installed on different systems (a **distributed installation**), but can be installed on the same system for small environments or demonstration purposes (a **single-system installation**).

**Figure 1. TE Console installation and upgrade steps**

```
New Installation

Configuring the TE Database (page 14)

Verify Requirements (page 25)

Install Java Components (page 26)

Install TE Console (page 27)

Upgrade

Is the current TE Console version 8.4.0 or later?

Y  Upgrading Tripwire Enterprise Console (page 33)

N  Upgrading Older Versions of Tripwire Enterprise (page 36)
```
Configuring the Tripwire Enterprise Database

Database Requirements

- For a list of supported backend databases for Tripwire Enterprise, see:
  http://www.tripwire.com/register/tripwire-enterprise-platform-and-device-support

- For hardware requirements for the database server, see:
  http://www.tripwire.com/register/the-tripwire-enterprise-hardware-configuration-parameters

- The database server must have a static IP address (non-DHCP), and a hostname that resolves to that address.

- The database server must provide a free port for communication with your TE Server. See Table 1 for details.

<table>
<thead>
<tr>
<th>Type of Database</th>
<th>Default Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>3306</td>
<td>TCP</td>
</tr>
<tr>
<td>Oracle</td>
<td>1521</td>
<td>TCP</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>1433</td>
<td>TCP</td>
</tr>
</tbody>
</table>

Table 1. Default ports and protocols for a remote database server

Database Installation & Configuration

Use the documentation provided by the database vendor to install your database.

After installing the database you plan to use with Tripwire Enterprise, see one of the following sections for configuration information:

- *Configuring a MySQL Database* (on the next page)
- *Configuring an Oracle Database* (on page 16)
- *Configuring a Microsoft SQL Server Database* (on page 17)

Note: TE Console requires that the passphrase used to connect to a database must be between 6 and 64 characters. Most ASCII printable characters are allowed, with a few exceptions:

- Alphanumeric characters (a-z, A-Z, 0-9), the space character (ASCII decimal 32), and most punctuation (\-_!@#$%^&*(),.+=[{}]|:/;?) are allowed.

- The single-quote (’), double-quote ("), less-than (<), greater-than (>), and backslash (\) characters are not allowed.
Configuring a MySQL Database

To use a MySQL database with Tripwire Enterprise, you must first configure the database so that Tripwire Enterprise can communicate with it.

**Note** You can configure MySQL to use SSL to secure communication with TE Console, but only after using the process below to initially connect to the Console. For more information about configuring SSL, see the Tripwire Enterprise Hardening Guide, available on the Downloads page of the Tripwire Customer Center.

To configure your MySQL database:

1. Open the MySQL configuration file on the database server in a text editor.

   **Tip** By default, the MySQL configuration files are:

   - **Linux or UNIX:** /etc/my.cnf
   - **Windows:** %PROGRAMDATA%\MySQL\MySQL Server <version>\my.ini

2. Add or change the following lines in the [mysqld] section of the configuration file:

   - `lower_case_table_names=1`
   - `max_allowed_packet=1G`

   **Caution** The `lower_case_table_names` value is a global setting for the MySQL database server, and will affect all databases hosted on that server.

3. Restart the MySQL service to implement the changes in the configuration file.

4. Open an SQL prompt on the database system and create the TE database:

   ```sql
   CREATE DATABASE <database_name> CHARACTER SET utf8 COLLATE utf8_bin;
   ```

5. Create a MySQL user account for TE Console, and provide access to the TE database.

   **If the database is on the same system as TE Console, run these commands:**

   ```sql
   CREATE USER '<user_name>'@'localhost' IDENTIFIED BY '<password>';  
   GRANT ALL PRIVILEGES ON <database_name>.* TO '<user_name>'@'localhost';
   ```

   **If the database is on a different system from TE Console, run these commands:**

   ```sql
   CREATE USER '<user_name>'@'<TE_Console_hostname>' IDENTIFIED BY '<password>';  
   GRANT ALL PRIVILEGES ON <database_name>.* TO '<user_name>'@'<TE_Console_hostname>';  
   ```

   **Caution** After TE Console connects to the MySQL database using this user account, the account cannot be deleted or TE Console will be unable to access the database again.

**Next** After configuring the database, proceed to *New Installations of Tripwire Enterprise Console* (on page 25).
Configuring an Oracle Database

To use an Oracle database with Tripwire Enterprise, you must first configure the database so that Tripwire Enterprise can communicate with it.

To configure your Oracle database, complete the following steps at an SQL prompt:

1. Create a tablespace for Tripwire Enterprise Console:

   CREATE TABLESPACE <tablespace_name>
   DATAFILE '<path_to_datafile_and_file_name>'
   SIZE 2000M
   AUTOEXTEND ON
   EXTENT MANAGEMENT LOCAL;

2. Create a user with access to the Tripwire Enterprise Console tablespace:

   CREATE USER <username>
   IDENTIFIED BY <password>
   DEFAULT TABLESPACE <tablespace_name>
   QUOTA UNLIMITED ON <tablespace_name>;

3. Grant the user the following privileges:

   GRANT CREATE VIEW, CREATE TABLE, ALTER SESSION, CREATE SESSION, CREATE SYNONYM, CREATE SEQUENCE, CREATE TRIGGER, CREATE PROCEDURE TO <username>;

Next  After configuring the database, proceed to New Installations of Tripwire Enterprise Console (on page 25).
Configuring a Microsoft SQL Server Database

To use an approved Microsoft SQL Server database with Tripwire Enterprise, complete the following steps:

- **Step 1 for MS SQL Server - Enable the TCP/IP protocol** (below)
- **Step 2 for MS SQL Server - Create the Remote Database** (on the next page)
- **Step 3 for MS SQL Server - Create a Login for the Remote Database** (on page 22)
- **Step 4 for MS SQL Server - Grant Database Permissions to the Login** (on page 24)

**Step 1 for MS SQL Server - Enable the TCP/IP protocol**

To enable TCP/IP on your Microsoft SQL Server database server:

1. From the Start menu, open **SQL Server Configuration Manager**.
2. In the tree pane, expand **SQL Server Network Configuration**, then click **Protocols for MSSQLSERVER** (see Figure 2 below).
3. In the main pane, select and enable the TCP/IP protocol.
4. In the tree pane, right-click **Protocols for MSSQLSERVER** and select **Properties**.
5. In the Flags tab of the properties dialog, determine if **ForceEncryption** (SSL) is enabled. If so, you will need to complete an additional step when you install TE Console (in *New Installations of Tripwire Enterprise Console* on page 25).
6. Close the SQL Server Configuration Manager.
7. Restart Microsoft SQL Server.

**Figure 2. Enabling the TCP/IP protocol**
Step 2 for MS SQL Server - Create the Remote Database

To create the Microsoft SQL Server database that will serve as your TE Console database:

1. In the Object Explorer of the Microsoft SQL Server Management Studio, right-click Databases and select New Database.

2. In the main pane of the New Database dialog (see Figure 3 below):
   a. Enter a Database Name.
   
   **Notes**  
   SQL Server database names are case-sensitive.  
   Make a note of the database name. You will need it to complete the Tripwire Enterprise Console Database installer.

   b. Enter at least 2000 MB as the Initial size of the data file.
   c. Enter at least 500 MB as the Initial size of the transaction log file.

Figure 3. Creating a new MS SQL database
3. Click the **Autogrowth** button for the data file, and complete the following steps in the Change Autogrowth dialog:
   
a. Select **Enable Autogrowth**.

   b. Enter appropriate settings (including at least 20 MB as the **File Growth** setting) and click **OK**.

   **Tip** To determine suitable autogrowth settings, consult your database administrator.

4. Click the **Autogrowth** button for the transaction log file, and complete the following steps in the Change Autogrowth dialog:
   
a. Select **Enable Autogrowth**.

   b. Enter appropriate settings (including at least 20 MB as the **File Growth** setting) and click **OK**.

5. In the New Database dialog, select **Options** (see **Figure 4** below).
   
a. In the **Collation** drop-down, select **Latin1_General_CS_AI**.

   b. In the **Recovery Model** drop-down, select **Simple**.

   c. In the **Miscellaneous** list, set the ANSI NULL Default value to True.

6. Click **OK** to close the New Database dialog.

**Figure 4. Configuring a new MS SQL database**
7. In the toolbar, click **New Query** (see Figure 5 below).

8. In the main pane, complete the following steps:

   a. In the new query tab, enter the following SQL statement:

   ```sql
   ALTER DATABASE [<db_name>] SET READ_COMMITTED_SNAPSHOT ON
   ```

   where `<db_name>` is the name of your database.

   **Tip** If the database name begins with a number, you must enclose the name of the database in quotes ("<db_name>").

   b. Click **Execute**, and verify that the command completed successfully.

   c. Enter the following statement in the query tab (see Figure 6 on the next page):

   ```sql
   SELECT name, is_read_committed_snapshot_on FROM sys.databases WHERE name='<db_name>'
   ```

   d. Click **Execute**.

   e. In the Results tab, verify that the value in the `is_read_committed_snapshot_on` column is 1. If this value is 0, repeat steps 8a through 8b above.

---

Figure 5. Setting READ_COMMITTED_SNAPSHOT ON

![Image showing setting READ_COMMITTED_SNAPSHOT ON](image-url)
Figure 6. Verifying that READ_COMMITTED_SNAPSHOT is on
Step 3 for MS SQL Server - Create a Login for the Remote Database

To create a Microsoft SQL Server login with which TE will access the remote database:

1. In the Object Explorer of the Microsoft SQL Server Management Studio, expand the Security folder (see Figure 7 on the next page).

2. Under the Security folder, right-click Logins and select New Login.

3. In the Login - New dialog:
   a. Enter a Login name.
   b. Select an authentication option.
   c. (SQL Server authentication only) Enter and confirm the password for the login.

   **Tip** Make a note of the login name and password. You will need it to complete the Tripwire Enterprise Console Database installer.

   d. (SQL Server authentication only) De-select Enforce password expiration.

   **Note** If this setting is enabled, then your SQL Server password might change. If the password changes, then you must reset the password with the TE Command Line Interface (CLI) in order to re-establish communication between the database and your Tripwire Enterprise Server. (For CLI instructions, see Working with the Command Line Interface in the Tripwire Enterprise Reference Guide).

   e. From the Default database drop-down, select the new SQL Server database.

   f. From the Default language drop-down, select English.

4. In the tree pane of the Login - New dialog, click User Mapping (see Figure 8 on the next page).
   a. Select the check box for the new database in the Map column.
   b. In the Default Schema column for the database, enter the name of the new login.

   **Caution** If you incorrectly enter the login name in the Default Schema column, an error may result when some Tripwire Enterprise functions are run.

   Do not assign a database role to the SQL Server login. If the login has a role, your Tripwire Enterprise Server may be unable to communicate with the database.

5. Click OK to close the Login - New dialog.
Figure 7. Creating a login for the remote database

Figure 8. Configuring user mapping
Step 4 for MS SQL Server - Grant Database Permissions to the Login

In this step, you grant permissions to the SQL Server login created for Tripwire Enterprise. Tripwire Enterprise needs these permissions to access the database via the SQL Server login.

To grant permissions in Microsoft SQL Server:

1. In the Object Explorer of the Microsoft SQL Server Management Studio, expand the Databases folder (see Figure 9 below).
2. Right-click the new database and select Properties.
3. In the database properties dialog, select Permissions.
4. In the main pane, select the Grant check box for each of the following permissions:
   - Connect
   - Create Procedure
   - Create Table
   - Create View
   - Delete
   - Insert
   - Select
   - Update
5. Click OK.

Figure 9. Granting database permissions to the login

Next After configuring the database, proceed to New Installations of Tripwire Enterprise Console (on the next page).
New Installations of Tripwire Enterprise Console

Step 1: Verify Hardware, Software, and Network Requirements

To verify that TE Console is supported on your system:

1. Check the list of supported operating systems for TE Console here:

   **Note**  
   TE Console can only be installed on a system with a 64-bit operating system.

2. Check the hardware requirements for the TE Server here:

3. Verify that all required ports are free on your Tripwire Enterprise Server.
   For a complete list, see *Tripwire Enterprise Console Services and Ports* on page 30.

4. The Tripwire Enterprise Server must reside on an IP network and have a static IP address (non-DHCP), as well as a hostname that resolves to the address.

5. Read the *Installation and Upgrade* section of the Release Notes ([release_notes.html](https://tripwireinc.force.com/customers)). The Release Notes are available for download from the Tripwire Customer Center ([https://tripwireinc.force.com/customers](https://tripwireinc.force.com/customers)).

   **Note**  
   The End-User License Agreement (EULA) includes all terms and conditions for the use of Tripwire Enterprise software. A hard copy of the EULA is provided in the packaging of Tripwire Enterprise Console. In addition, the Tripwire Enterprise installation DVD and electronic downloads include a soft copy of the EULA ([license.html](https://tripwireinc.force.com/customers)).

   Prior to installing Tripwire Enterprise Console, you should first read the EULA in its entirety. **Installation of Tripwire Enterprise Console software implies your consent to all terms and conditions outlined in the EULA.**
Step 2: Install Java Components

Java SE 8 JRE and the Java Cryptography Extension (JCE) files must be installed on the target system before installing TE Console.

To download and install the JRE and JCE files:

1. Navigate to the Java SE Downloads section of the Oracle website:

2. Download the following files:
   - the Java SE 8 Java Runtime Environment (JRE)
   - the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 8

   **Note**  For information on supported versions of the JRE and JCE, see the Installation and Upgrade section of the Release Notes (release_notes.html). The Release Notes are available for download from the Tripwire Customer Center (https://tripwireinc.force.com/customers).

3. Follow these instructions to install the JRE on your TE Server system:
   http://docs.oracle.com/javase/8/docs/technotes/guides/install/install_overview.html

   Make a note of where the JRE is installed for the next step.

4. Install the JCE policy files:
   a. Uncompress and extract the JCE file you downloaded.
   b. Copy the extracted local_policy.jar and US_export_policy.jar files to <java_home>/lib/security, overwriting the existing files with the same names.
Step 3: Install Tripwire Enterprise Console

To install TE Console for the first time:

1. For Linux systems, create a user group and user account for the installer on the system where you want to install TE Console:
   
a. Log in with root privileges.
   
b. At a command prompt, enter the following command to create a group (called `tripwire`) with a unique group ID:
      
      `groupadd tripwire`
   
c. Enter the following command to create a new user (called `tripwire`) in the `tripwire` group.
      
      `useradd -M -g tripwire tripwire`

For Windows systems, log in to the TE Server with Administrator privileges.

2. Access your Tripwire Enterprise installation DVD or download archive.

3. Navigate to the installer directory for your platform and enter the installer command (see Table 2).

Table 2. TE Console installer directories and commands

<table>
<thead>
<tr>
<th>Platform</th>
<th>Installer Directory</th>
<th>Installer Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>server/linux</td>
<td>./install-server-linux-amd64.bin</td>
</tr>
<tr>
<td>Windows</td>
<td>server\windows</td>
<td>install-server-windows-amd64.exe</td>
</tr>
</tbody>
</table>

Note: **Console mode** installs your Tripwire Enterprise Console software with a command-line interface. Console mode is not available for Windows installations, and runs by default if you are logged into a terminal session on a Linux system without X Windows support.

To force the installer to use console mode on a Linux system with X Windows support, add a --mode text flag to the installer command. For example:

```
./install-server-linux-amd64.bin --mode text
```

To complete the command-line installer, follow the on-screen instructions.

4. In the installer, select the version of the JRE that you want TE Console to use. If an installed version of the JRE is not listed, set the JAVA_HOME environment variable to the JRE directory’s path and restart the installer.

5. Follow the on-screen instructions to complete the installation. The installation process may take several minutes.

For successful installations, the installation log file is written to `<te_root>/server/data/log/install-<version>.log`. 
For failed installations, the log file is written to one of the following locations:

**Linux**: /tmp/bitrock_installer_<proc_ID>.log  
**Windows**: C:\Users\<user>\AppData\Local\Temp\bitrock_installer_<proc_ID>.log

6. At the end of the installation process, the installer can open a browser to continue configuring Tripwire Enterprise.

   - **If you have a Microsoft SQL Server database and you want to use SSL to secure communication**, do not launch a browser yet. Clear the check box, click **Finish**, and complete step 7 below.
   - **Otherwise**, click **Finish** and skip to step 8.

7. **To configure SSL for a Microsoft SQL Server database**, complete the following steps:

   a. If the database server uses a self-signed certificate or a certificate issued by a trusted authority that is not supported by the JRE, you must add the certificate to the keystore on the TE Server. To do so, run the following command at a command prompt on the TE Server:

   `<JAVA_HOME>\bin\keytool -import -alias <alias> -keystore <te_root>\server\data\security\customer_trust_store.ks -file <cert>

   where
   - `<JAVA_HOME>` is the Java directory specified during TE Console installation,
   - `<alias>` is any unique identifier for the new keystore entry,
   - `<te_root>` is the installation directory for Tripwire Enterprise software, and
   - `<cert>` is the path to the certificate

   b. Enter changeit when prompted for the keystore passphrase.

   c. If you added a certificate to the TE Server keystore in step 7a, you must restart the TE Console service in order to force TE Console to re-read the keystore file:

   `<te_root>\Server\bin\twservices restart`

8. If the TE installer does not automatically launch a browser, open a Web browser and enter the following URL:

   https://<TE_Server>

   where `<TE_Server>` is the hostname or IP address of the TE Console system. If you changed the default Web Services port during the TE Console installation, use:

   https://<TE_Server>:\<port>

**Notes**

For the list of supported browsers, see:  
http://www.tripwire.com/it-security-software/scm/specifications/system-requirements

For all browsers, TLS (TLSv1, TLSv1.1, or TLSv1.2), Javascript, and cookies must be enabled.
9. Enter the services passphrase to access a database configuration dialog. Enter the
database information and restart TE.

10. Enter the services passphrase again to change the default passphrase for the
    TE administrator user account.

11. Log in to TE using the administrator account you just created. Use the Fast Track
    interface to configure Tripwire Enterprise and create a personal user account. At the end
    of Fast Track, you will be logged into TE using this account.

Next  To begin using TE Console, see the Tripwire Enterprise User Guide. A PDF version
       is available in the docs directory on the Tripwire Enterprise installation DVD. You
       can also view User Guide content in the online help, which can be accessed by
       clicking Help in any Tripwire Enterprise Manager.

       For more information about configuring and maintaining your Tripwire Enterprise
       implementation, see:

       • Chapter 4: Post-Installation Configuration (on page 113)
       • Chapter 5: Maintenance Procedures (on page 121)
       • The Tripwire Enterprise Hardening Guide, available from the Downloads
         page of the Tripwire Customer Center (www.tripwire.com/customers).
Tripwire Enterprise Console Services and Ports

The tables in this section list the services installed with Tripwire Enterprise Console, and the default ports used. Figure 10 on page 32 illustrates these connections.

For more information about services and ports used by Tripwire Enterprise, see:

- Database Requirements (on page 14)
- Services Installed with Tripwire Enterprise Agent on page 42
- Requirements for a Tripwire Enterprise Agent System (on page 43)
- Configuring a Tripwire Enterprise Proxy for Agent Communication (on page 117)

### Table 3. Services installed with Tripwire Enterprise Console on Linux systems

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Listening Ports</th>
<th>Requires Firewall Access?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>twservices</td>
<td>443</td>
<td>Y</td>
<td>End user web UI</td>
</tr>
<tr>
<td>8080</td>
<td>Y</td>
<td></td>
<td>HTTP/EMS integration services</td>
</tr>
<tr>
<td>9898</td>
<td>Y</td>
<td></td>
<td>Incoming RMI from TE Agents</td>
</tr>
<tr>
<td>9899</td>
<td>N</td>
<td></td>
<td>Incoming RMI from TE Console</td>
</tr>
<tr>
<td>69</td>
<td>Y</td>
<td></td>
<td>Network device TFTP</td>
</tr>
<tr>
<td>61616</td>
<td>N</td>
<td></td>
<td>ActiveMQ message broker</td>
</tr>
<tr>
<td>twrtmd</td>
<td>1169</td>
<td>N</td>
<td>TE Agent event queue</td>
</tr>
</tbody>
</table>

### Table 4. Services installed with Tripwire Enterprise Console on Windows systems

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Listening Ports</th>
<th>Requires Firewall Access?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tripwire Enterprise Server</td>
<td>443</td>
<td>Y</td>
<td>End user web UI</td>
</tr>
<tr>
<td>8080</td>
<td>Y</td>
<td></td>
<td>HTTP/EMS integration services</td>
</tr>
<tr>
<td>9898</td>
<td>Y</td>
<td></td>
<td>Incoming RMI from TE Agents</td>
</tr>
<tr>
<td>69</td>
<td>Y</td>
<td></td>
<td>Network device TFTP</td>
</tr>
<tr>
<td>61616</td>
<td>N</td>
<td></td>
<td>ActiveMQ message broker</td>
</tr>
<tr>
<td>Tripwire Enterprise Agent</td>
<td>9899</td>
<td>N</td>
<td>Incoming RMI from TE Console</td>
</tr>
<tr>
<td>Tripwire Detection Service</td>
<td>1169</td>
<td>N</td>
<td>TE Agent event queue</td>
</tr>
</tbody>
</table>
Table 5. Required ports for a Tripwire Enterprise Server

<table>
<thead>
<tr>
<th>Default Port/Protocol</th>
<th>Configurable During Installation?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>69/UDP</td>
<td>No</td>
<td>Used for inbound communication received from network devices that support TFTP.</td>
</tr>
<tr>
<td>443/TCP</td>
<td>Yes</td>
<td>Used for Tripwire Enterprise interface sessions (HTTPS) initiated by Tripwire Enterprise users. For 8.3.3 - 8.4.0 TE Agents, used to connect to the TE Console for an RMI SSL certificate signing request only when FIPS mode is enabled on both TE Console and TE Agent. For more information on FIPS, see the <em>Tripwire Enterprise Hardening Guide</em>, available for download from the Tripwire Customer Center.</td>
</tr>
<tr>
<td>8080/TCP</td>
<td>Yes</td>
<td>Used for download of JAR files to TE Agent systems, as well as external integrations such as plug-ins (HTTP). For 8.4.1 and later TE Agents, used to connect to the TE Console for an RMI SSL certificate signing request.</td>
</tr>
<tr>
<td>9898/TCP</td>
<td>Yes</td>
<td>Used for inbound communication received from Tripwire Enterprise Agents.</td>
</tr>
</tbody>
</table>

Table 6. Optional outbound ports for a Tripwire Enterprise Server

<table>
<thead>
<tr>
<th>Default Port/Protocol</th>
<th>Configurable During Installation?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>25/TCP</td>
<td>No</td>
<td>Used for outbound e-mail (SMTP) sent by Tripwire Enterprise e-mail actions. You can configure this port when you create or modify an e-mail server in the Tripwire Enterprise interface. For more information, see What are E-mail Servers? in the <em>Tripwire Enterprise User Guide</em>.</td>
</tr>
<tr>
<td>162/UDP</td>
<td>No</td>
<td>Used for outbound SNMP traps sent by Tripwire Enterprise SNMP actions. For more information, see How Does an SNMP Action Work? in the <em>Tripwire Enterprise User Guide</em>.</td>
</tr>
<tr>
<td>514/UDP</td>
<td>No</td>
<td>Used for outbound syslog notifications sent by Tripwire Enterprise syslog actions. For more information, see What are Actions and Action Types? in the <em>Tripwire Enterprise User Guide</em>.</td>
</tr>
</tbody>
</table>

**Note** A network device may employ one or more of the ports depicted in Figure 10 on the next page. If a port will not be used in your Tripwire Enterprise implementation, you can close the port on any existing firewalls. For example, if Tripwire Enterprise will not monitor any network devices, you can close port 69 on your firewall.
Figure 10. Tripwire Enterprise port configuration

Note: All communication conducted via TCP, unless otherwise noted.
Upgrading Tripwire Enterprise Console

Use this procedure to upgrade Tripwire Enterprise Console 8.4.0 or later to version 8.5.x.

Caution
The TE Console 8.5.x installer can only upgrade TE Console 8.4.0 or later. To upgrade an earlier version of the software, you must first migrate to TE Console version 8.4. For more information, see Upgrading Older Versions of Tripwire Software (on page 36).

Step 1: Verify Hardware and Software Requirements

To verify that TE Console is supported on your system:

1. Check the list of supported operating systems for TE Console here:

   http://www.tripwire.com/it-security-software/scm/specifications/system-requirements

2. Check the hardware requirements for the TE Server here:

   http://www.tripwire.com/register/the-tripwire-enterprise-hardware-configuration-parameters


Step 2. Back Up Data and Configuration Files

Before upgrading, back up the data in your Tripwire Enterprise database. The installer will migrate existing TE data for use with version 8.5.x, but you should create a backup in case there is a problem during the upgrade process. The TE configuration files store important information about your TE Console installation, and should also be backed up at this time.

To back up Tripwire Enterprise data and configuration files:

1. Back up the data in your Tripwire Enterprise database. For specific backup instructions, consult your database documentation.

   To back up the embedded MySQL database in an existing TE Console, see Backing Up and Restoring Tripwire Enterprise in the Tripwire Enterprise Installation & Maintenance Guide that came with the installed version of TE Console.

2. On the TE Console system, use the following command to back up the TE configuration files:

   <te_root>/server/bin/tetool backup --passphrase <services_passphrase> <output_config_filename>

   For more information on the tetool backup command, see Backing Up Tripwire Enterprise Data and Configuration Files on page 123.
Step 3. Upgrade Tripwire Enterprise Console

In this step, the TE Console installer upgrades your current installation to the latest version.

To run the installer:

1. Log in to your Tripwire Enterprise Server with root or Administrator privileges.
2. Access your Tripwire Enterprise installation DVD or download archive.
3. Navigate to the installer directory for your platform and enter the installer command (see Table 7).
4. The installer will detect the existing version of Tripwire Enterprise, and ask you if you want to upgrade. Click Yes to confirm.
5. Select the version of the JRE that you want the TE Console to use. If an installed version of the JRE is not listed, set the JAVA_HOME environment variable to the JRE directory’s path and restart the installer.
6. Follow the on-screen instructions to complete the upgrade. The upgrade process may take some time, based on the size of your database.

For successful upgrades, the installation log file is written to &lt;te_root&gt;/server/data/log/install-&lt;version&gt;.log.

For failed upgrades, the log file is written to one of the following locations:

   Linux: /tmp/bitrock_installer_<proc_ID>.log
   Windows: C:\Users\&lt;user&gt;\AppData\Local\Temp\bitrock_installer_<proc_ID>.log

7. Clear your Web browser’s temporary file cache, then log in to TE Console.

Table 7. TE Console installer directories and commands

<table>
<thead>
<tr>
<th>Platform</th>
<th>Installer Directory</th>
<th>Installer Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>server/linux</td>
<td>./install-server-linux-amd64.bin</td>
</tr>
<tr>
<td>Windows</td>
<td>server\windows</td>
<td>install-server-windows-amd64.exe</td>
</tr>
</tbody>
</table>

Note: Console mode installs your Tripwire Enterprise Console software with a command-line interface. Console mode is not available for Windows installations, and runs by default if you are logged into a terminal session on a Linux system without X Windows support.

To force the installer to use console mode on a Linux system with X Windows support, add a --mode text flag to the installer command. For example:

   ./install-server-linux-amd64.bin --mode text

To complete the command-line installer, follow the on-screen instructions.
Step 4. Restart Tripwire Enterprise Agents

After upgrading TE Console, you should restart the TE Agent software on all systems monitored by that Console to sync them with the new installation. You can restart all TE Agents at once or do it over time, but all Agents should be restarted after an upgrade.

To restart Tripwire Enterprise Agents:

1. Log in to TE Console.
2. Restart all Tripwire Enterprise Agents:
   a. Click NODES, then select the Asset View tab.
   b. Select the assets to restart, then click Health Check > Restart at the top of the right pane.

Note When Tripwire Enterprise restarts a TE Agent, the Log Manager generates a System log message that states:

   Finished recreating data on Node <node_name>.

After Upgrading

After upgrading your TE Console installation, you may need to perform some additional steps:

- For information on hardening your Tripwire Enterprise installation, see the Tripwire Enterprise Hardening Guide, available for download from the Tripwire Customer Center.

- If you are upgrading a single-system Tripwire Enterprise installation with an embedded MySQL database, we recommend that you upgrade the database after successfully upgrading TE Console. For information on migrating to a newer version of MySQL, see the TE Documentation section on the Downloads page of the Tripwire Customer Center.

- If your previous Tripwire Enterprise implementation included policy tests, and you want to import the latest policy files from the Tripwire Web site, see What are Pre-Configured Rules and Policies? in the Tripwire Enterprise User Guide.

- If you upgrade a Tripwire Enterprise implementation that includes custom user roles, you should review the permissions in each role following upgrade. In some cases, custom user roles may require new permissions for expected access to Tripwire Enterprise objects and functions. For more information about user roles and permissions, see What are User Permissions and User Roles? in the Tripwire Enterprise User Guide.
Upgrading Older Versions of Tripwire Software

The Tripwire Enterprise 8.5.x Console installer can only upgrade TE Console version 8.4.0 or later. To upgrade a TE Console installation that is older than Tripwire Enterprise 8.4, follow the applicable upgrade path in Table 8 below.

Tips
You can download the TE Console installers and documentation from the Downloads page of the Tripwire Customer Center at http://tripwire.com/customers.

TE Agents older than version 8.3.7 on AIX and Linux PowerPC platforms will be unable to connect to TE Console 8.4 or later. We recommend that you upgrade these Agents to version 8.3.7 or later before upgrading TE Console to version 8.4. To upgrade these Agents after TE Console 8.4.0 is installed, first uninstall the older version of TE Agent (retaining any residual files), then perform a new installation of TE 8.4 Agent.

If you upgrade a Tripwire Enterprise implementation that includes custom user roles, you should review the permissions in each role following upgrade. In some cases, custom user roles may require new permissions for expected access to Tripwire Enterprise objects and functions. For more information about user roles and permissions, see What are User Permissions and User Roles? in the Tripwire Enterprise User Guide.

Table 8. Upgrade paths for Tripwire Enterprise Console

<table>
<thead>
<tr>
<th>Tripwire Enterprise Version</th>
<th>Upgrade Path</th>
</tr>
</thead>
</table>
| 7.6                         | 1. TE Console 8.0  
2. TE Console 8.2  
3. TE Console 8.4  
4. See Upgrading Tripwire Enterprise Console on page 33. |
| 7.7                         | 1. TE Console 8.1  
2. TE Console 8.3  
3. TE Console 8.4  
4. See Upgrading Tripwire Enterprise Console on page 33. |
| 8.0                         | 1. TE Console 8.2  
2. TE Console 8.4  
| 8.1                         | 1. TE Console 8.2  
2. TE Console 8.4  
| 8.2 or later                | 1. TE Console 8.4  
2. See Upgrading Tripwire Enterprise Console on page 33. |
Uninstalling Tripwire Enterprise Console

With the following procedures, you can remove Tripwire Enterprise Console software from your Tripwire Enterprise Server.

An uninstall log will be written to one of the following locations:

**Linux:** /tmp/bitrock_installer_<proc_ID>.log  
**Windows:** C:\Users\<user>\AppData\Local\Temp\bitrock_installer_<proc_ID>.log

**To uninstall Tripwire Enterprise Console software via command line:**

1. Log in to your Tripwire Enterprise Server with root or Administrator privileges.

2. At a command prompt, enter:
   
   cd <te_root>/server/uninstall
   
   where <te_root> is the path to the directory in which TE Console is installed.

   **Note** By default, TE Console is installed in the following directories.

   **Windows:** C:\Program Files\Tripwire\TE  
   **Linux:** /usr/local/tripwire/te

3. To run the uninstaller on a Linux system, enter:

   ./uninstall

   To run the uninstaller on a Windows system, enter:

   uninstall.exe

4. Manually delete the TE Console installation directory (<te_root>) and its contents.

**To uninstall TE Console from a Windows TE Server with the Windows Start menu:**

1. Click **Start** and select the correct path for your platform:

   Programs > Tripwire Enterprise Console > Uninstall

   All Programs > Tripwire Enterprise Console > Uninstall

2. Follow the prompts in the uninstaller.

3. Manually delete the TE Console installation directory and all contents.
To uninstall TE Console from a Windows TE Server with the Add/Remove Programs feature:

1. Log in to your Tripwire Enterprise Server with Administrator privileges.
2. From the Control Panel, select Add/Remove Programs.
4. Click Remove.
5. Follow the prompts in the uninstaller.
6. Manually delete the TE Console installation directory and all contents.
Chapter 2. Installing Tripwire Enterprise Agent
Installation Requirements for Tripwire Enterprise Agent

Tripwire Enterprise Agent (TE Agent) is a remote-execution environment that enables Tripwire Enterprise Console to monitor a file server for changes. When you install TE Agent on a file server, TE automatically creates a file server node (or Agent node) in the Node Manager.

- For more information about creating file server nodes, see Creating a Node by Installing Agent Software in the Tripwire Enterprise User Guide.
- To learn how other types of nodes are created, see Creating a Node Manually in the Tripwire Enterprise User Guide.

Note Tripwire Enterprise Agent and Tripwire Axon Agent (Axon Agent) cannot be installed on the same system. You must manually uninstall TE Agent from a system before installing Axon Agent. For more information, see Uninstalling Tripwire Enterprise Agent on page 79.

About Interactive and Silent Installations

Tripwire Enterprise Agent can be installed with either of the following methods:

- With an interactive installation, you launch and complete the Tripwire Enterprise Agent installer. In the installer, you respond to a series of questions and enter configuration settings.
- With a silent installation, you use a command line or response file to automate the installation process.

The End-User License Agreement

The End-User License Agreement (EULA) includes all terms and conditions for the use of Tripwire Enterprise software. A hard copy of the EULA is provided in the packaging of Tripwire Enterprise Console. In addition, your Tripwire Enterprise installation DVD or electronic download includes a soft copy of the EULA (license.html).

Prior to installing Tripwire Enterprise Agent, you should first read the EULA in its entirety. Installation of TE Agent software implies your consent to all terms and conditions outlined in the EULA.
Preparing for Tripwire Enterprise Agent Installation

Prior to installing Tripwire Enterprise Agent, complete the following steps:

- Install the Tripwire Enterprise Console software and database, as described in Chapter 1: Installing Tripwire Enterprise Console (on page 12).
- Ensure that the TE Agent host system complies with all requirements (see Requirements for a Tripwire Enterprise Agent System on page 43).

**Caution** For a successful installation, a TE Agent host system must be in compliance with all requirements. If the host system does not meet all requirements, your installation may fail.

Once all requirements have been fulfilled, proceed to the appropriate section for your platform:

- Installing Tripwire Enterprise Agent on AIX (on page 44)
- Installing Tripwire Enterprise Agent on Apple OS X (on page 49)
- Installing Tripwire Enterprise Agent on HP-UX (on page 53)
- Installing Tripwire Enterprise Agent on Linux (on page 57)
- Installing Tripwire Enterprise Agent on Solaris (on page 61)
- Installing Tripwire Enterprise Agent on Windows (on page 67)
Services Installed with Tripwire Enterprise Agent

The tables in this section list the services installed with Tripwire Enterprise Agent. For information on the services installed with Tripwire Enterprise Console, see *Tripwire Enterprise Console Services and Ports on page 30*.

Table 9. Services installed with Tripwire Enterprise Agent software

<table>
<thead>
<tr>
<th>TE Agent Platform</th>
<th>Service Name</th>
<th>Listening Ports</th>
<th>Requires Firewall Access?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>teagent</td>
<td>9898</td>
<td>Y</td>
<td>Incoming RMI from TE Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1080</td>
<td>Y</td>
<td>Used only if the TE Agent is a SOCKS proxy</td>
</tr>
<tr>
<td></td>
<td>teeg</td>
<td>1169</td>
<td>N</td>
<td>TE Agent event queue</td>
</tr>
<tr>
<td></td>
<td>teges</td>
<td>none</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-UX</td>
<td>TWeagent</td>
<td>9898</td>
<td>Y</td>
<td>Incoming RMI from TE Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1080</td>
<td>Y</td>
<td>Used only if the TE Agent is a SOCKS proxy</td>
</tr>
<tr>
<td>Linux</td>
<td>twdaemon</td>
<td>9898</td>
<td>Y</td>
<td>Incoming RMI from TE Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1080</td>
<td>Y</td>
<td>Used only if the TE Agent is a SOCKS proxy</td>
</tr>
<tr>
<td></td>
<td>twrtmd</td>
<td>1169</td>
<td>N</td>
<td>TE Agent event queue</td>
</tr>
<tr>
<td>OS X</td>
<td>Tripwire Enterprise Agent</td>
<td>9898</td>
<td>Y</td>
<td>Incoming RMI from TE Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1080</td>
<td>Y</td>
<td>Used only if the TE Agent is a SOCKS proxy</td>
</tr>
<tr>
<td></td>
<td>Tripwire Event Generator</td>
<td>1169</td>
<td>N</td>
<td>TE Agent event queue</td>
</tr>
<tr>
<td>Solaris</td>
<td>twdaemon</td>
<td>9898</td>
<td>Y</td>
<td>Incoming RMI from TE Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1080</td>
<td>Y</td>
<td>Used only if the TE Agent is a SOCKS proxy</td>
</tr>
<tr>
<td></td>
<td>teeg</td>
<td>1169</td>
<td>N</td>
<td>TE Agent event queue</td>
</tr>
<tr>
<td></td>
<td>teges</td>
<td>none</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td>Tripwire Enterprise Agent</td>
<td>9898</td>
<td>Y</td>
<td>Incoming RMI from TE Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1080</td>
<td>Y</td>
<td>Used only if the TE Agent is a SOCKS proxy</td>
</tr>
<tr>
<td></td>
<td>Tripwire Detection Service</td>
<td>1169</td>
<td>N</td>
<td>TE Agent event queue</td>
</tr>
</tbody>
</table>
Requirements for a Tripwire Enterprise Agent System

Prior to installing Tripwire Enterprise Agent software, you should first ensure that each host system complies with the requirements in the following sections:

- Supported Platforms (below)
- Network Requirements (below)
- Additional Requirements for Specific Platforms (below)

Supported Platforms

The Tripwire Web site provides current information on:

- The operating systems on which Tripwire Enterprise Agent software may be installed.
- The operating systems on which the Tripwire Enterprise Event Generator can be installed. An Event Generator is required for real-time monitoring of a TE Agent system, and can also be used to collect audit event information. When you run the TE Agent installer on a supported Solaris system, an Event Generator is automatically installed. For all other supported platforms, the installer gives you the option of installing an Event Generator.

For further details, see:

http://www.tripwire.com/register/tripwire-enterprise-platform-and-device-support

Network Requirements

To install Tripwire Enterprise Agent, the host system must provide a free port to listen for communications from your Tripwire Enterprise Server. Port 9898 is the default setting.

| Note | If needed, you can change the communication port after installation of Tripwire Enterprise Agent. To do so, edit the following line in the TE Agent properties file (<te_root>/agent/data/config/agent.properties):
|      | tw.local.port=<communication_port> |
|      | For a diagram of default ports that may be involved in a Tripwire Enterprise implementation, see Figure 10 on page 32. |

Additional Requirements for Specific Platforms

To install TE Agent on an AIX system, the system must have at least AIX 5.3 Technology Level 9 and Patch Level 2. To validate these requirements, run oslevel -s. The return value should be 5300-09-02-0849 or higher.

To install TE Agent on a Solaris or HP-UX system, you must first install all required patches for the platform.
Installing Tripwire Enterprise Agent

Installing Tripwire Enterprise Agent on AIX

The AIX version of the Tripwire Enterprise Agent installer is a native RPM package. The native RPM package and usage license are embedded in the delivered binary file (te_agent.bin).

The AIX Event Generator utilizes native OS auditing as its event source. TE edits both the bin and stream commands of the audit system to include Tripwire's event filter, so that events that are only of interest to Tripwire are filtered from the audit log of the system. This allows you to continue to use auditing normally in parallel with Tripwire's monitoring.

The TE Agent installer can configure the native OS auditing during installation, or after installation you can run the configuration script (found in <te_root>/agent/sup/rtm with the other real-time monitoring components) manually.

To install Tripwire Enterprise Agent on an AIX system, see:

- *Interactive Installation for AIX* (below)
- *Silent Installation for AIX* (on page 46)

Interactive Installation for AIX

To interactively install Tripwire Enterprise Agent on an AIX system:

1. Log in to the system with root privileges.

2. For a DVD installation, copy the following file from the Tripwire Enterprise installation DVD to a temporary directory on the local drive:

   te_agent/aix/te_agent.bin

   For a download installation, expand the download file to a temporary directory on the local drive.

3. To install the software in the default installation directory

   (/usr/local/tripwire/te/agent), launch the installer by entering the following command at a command prompt:

   ./te_agent.bin

   To install the software in a different directory, add the **--install-dir** option as follows:

   ./te_agent.bin --install-dir <installation_directory>

**Note** If you install the software in a directory other than the default location, make a note of it. You will need the full path to start the Agent.
4. If AIX is not already configured for auditing, the installer will prompt:

   Audit configuration should take place so that real time will work. Do you want to allow audit configuration? [y/N]

   Enter y. If you want to configure auditing after installation, enter N.

5. If either binmode and streammode are set to on in the audit configuration file, the installer will prompt you to either leave these settings on or turn them off. Tripwire recommends setting both of these to off, unless they are required for non-TE OS auditing.

   If binmode and streammode are set to off in the audit configuration file, installation will complete normally.

6. If you chose not to configure auditing in step 4, you should configure it now. For more information on this process, see Post-Installation Audit Configuration on page 48.

7. If the TE Console you will use to manage this Agent uses a non-default HTTP port (the default port is 8080), you must edit the Agent's properties file to specify it:

   a. On the TE Agent system, open `<te_root>/agent/data/config/agent.properties` in a text editor.

   b. Add the following line, overwriting any existing `webserver.http.port` value:

      ```
      webserver.http.port=<Console_HTTP_port>
      ```

      The Console's HTTP port is the value of the `webserver.http.port` property, specified in the `server.properties` file on the TE Console system.

   c. Save the file.

8. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See Using Tag Files to Assign Tags to New TE Agents on page 72 for more information.

   Follow these steps to create a tag file:

   a. Create a text file named `agent.tags.conf` with the tags that you want to assign.

   b. Copy the tag file to `<te_root>/agent/data/config` on the TE Agent system.

9. Start the TE Agent. For instructions, see Managing the Tripwire Enterprise Agent Service on page 134.

---

**Next**  For information on hardening your Tripwire Enterprise Agent installation, see the Tripwire Enterprise Hardening Guide, available for download from the Tripwire Customer Center.
Silent Installation for AIX

**Note** By installing Tripwire Enterprise Agent software, you consent to all terms and conditions outlined in the Tripwire EULA. For more information, see *The End-User License Agreement* on page 40.

To silently install Tripwire Enterprise Agent on an AIX system:

1. Log in to the system with root privileges.
2. For a DVD installation, copy the following file from the Tripwire Enterprise installation DVD to a temporary directory on the local drive:
   
   `te_agent/aix/te_agent.bin`

   For a download installation, expand the file to a temporary directory on the local drive.
3. To install the software in the default installation directory
   (`/usr/local/tripwire/te/agent`), launch the installer by entering the following command at a command prompt:

   ```bash
   ./te_agent.bin --eula accept --silent --server-host <server_host>
   --server-port <server_port> --passphrase <services_password>
   --rtmport <port number> --enable-audit-conf <true|false>
   --turn-bin-mode-off <true|false> --turn-stream-mode-off <true|false>
   ```

   To install the software in a different directory, add the following option:
   
   ```bash
   --install-dir <installation_directory>
   ```

   For command-line component definitions, see Table 10 on the next page.

   **Note** If you install the software in a directory other than the default location, make a note of it. You will need the full path to start the Agent.

4. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See *Using Tag Files to Assign Tags to New TE Agents* on page 72 for more information.

   Follow these steps to create a tag file:
   
   a. Create a text file named `agent.tags.conf` with the tags that you want to assign.
   
   b. Copy the tag file to `<te_root>/agent/data/config` on the Agent system.

5. Start the Agent. For instructions, see *Managing the Tripwire Enterprise Agent Service* on page 134.
<table>
<thead>
<tr>
<th>Command-line Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--eula accept</td>
<td>Indicates your agreement with the Tripwire EULA.</td>
</tr>
</tbody>
</table>
| --enable-audit-conf <true|false> | (Optional) Tells the installer to configure AIX for auditing. If set to false, you must manually configure auditing after the installation. For more information, see Post-Installation Audit Configuration on the next page.  
  **Note:** This setting must be used in conjunction with the --rtmport, --turn-bin-mode-off, and --turn-stream-mode-off settings. |
| --enable-fips          | (Optional) Enables FIPS mode for the TE Agent.  
  **Note:** For information on FIPS mode, see the Tripwire Enterprise Hardening Guide, available for download from the Tripwire Customer Center. |
| --http-port <http_port> | (Optional) If your TE Console is using a non-default HTTP port (8080 is the default), you must use this option to specify the HTTP port. |
| --install-dir <installation_directory> | (Optional) The full path to a non-default installation directory. |
| --passphrase <services_password> | The same Services Password entered when Tripwire Enterprise Console was installed. |
| --proxy-host <proxy_host> | (Optional) The hostname or IP address of a Tripwire Enterprise proxy. |
| --proxy-port <proxy_port> | (Optional) The number of the port on a Tripwire Enterprise proxy with which TE will communicate with the proxy.  
  **Note:** For more information about proxies, see Configuring a Tripwire Enterprise Proxy for Agent Communication on page 117. |
| --rtmport <port number> | (Optional) The real-time monitoring port (1169 by default).  
  **Note:** This setting must be used in conjunction with the --enable-audit-conf, --turn-bin-mode-off, and --turn-stream-mode-off settings. |
| --server-host <server_host> | The hostname or IP address of your Tripwire Enterprise Server. |
| --server-port <server_port> | The number of the services port on your Tripwire Enterprise Server (9898 by default).  
  **Note:** You specified the services port when you installed Tripwire Enterprise Console. The Tripwire Enterprise Server communicates with all TE Agents via the services port. |
| --tmp-dir <temporary_directory> | (Optional) Specifies an alternative temporary directory for the installation. |
**Command-line Component** | **Description**
--- | ---
--turn-bin-mode-off <true|false> | (Optional) Turns AIX auditing binmode on or off. Tripwire recommends setting this to true (unless binmode is required for non-TE OS Auditing).

**Note:** This setting must be used in conjunction with the --enable-audit-conf, --rtmport, and --turn-stream-mode-off settings.

--turn-stream-mode-off <true|false> | (Optional) Turns AIX Auditing streammode on or off. Tripwire recommends setting this to true (unless streammode is required for non-TE OS Auditing).

**Note:** This setting must be used in conjunction with the --enable-audit-conf, --turn-bin-mode-off, and --rtmport settings.

**Post-Installation Audit Configuration**

If you did not configure AIX audit configuration during the TE Agent installation process, run the following script from the command line of the AIX Agent system:

```
<te_root>/agent/sup/rtm/teauditconfig
```

If either binmode or streammode are on, you will be prompted to either leave them on or turn them off. Tripwire recommends turning these off, unless they are required for non-TE OS auditing.

**Restoring Audit Configuration Files**

When TE Agent is installed on an AIX system, it changes some AIX audit configuration files (bincmds, config, and streamcmds) and creates backup copies of the originals. The backup files have a date stamp appended to the filename (for example, bincmds.25-Mar-2011-05.42.27).

If you uninstall TE Agent or want to disable real-time monitoring, you should restore the modified audit configuration files using the backup copies.

**To restore your audit configuration files:**

1. Log in to the AIX system with root privileges.
2. Enter the following command:
   ```
   cd /etc/security/audit
   ```
3. Use commands like the following to restore the bincmds, config, and streamcmds files:
   ```
   a. mv bincmds bincmds.tw
   b. mv bincmds.<datestamp> bincmds
   ```
4. Review the contents of each file to verify that it is correct.
Installing Tripwire Enterprise Agent on Apple OS X

The OS X version of the Tripwire Enterprise Agent installer is available in two forms:

- a **text-based command line installer** (`te_agent.bin`), a native OS X package with the package and usage license embedded in the binary file
- a **GUI installer/configuration tool** (`te_agent.dmg`), a native OS X disk image file that contains the TE Agent installer app. The package and usage license are embedded in the app file (`Tripwire Enterprise Agent.app`).

To install Tripwire Enterprise Agent on an OS X system, see:

- *Interactive Installation for OS X* (below)
- *Silent Installation for OS X* (on page 51)

### Interactive Installation for OS X

**Note**  Java Runtime Environment (JRE) version 1.6.0_37 or later must be installed on an OS X system before TE Agent can be installed. For information on installing a JRE, see your OS X system documentation or contact Apple Support.

**To interactively install Tripwire Enterprise Agent on an OS X system:**

1. Log in to the system with root privileges.
2. For a DVD installation, copy the appropriate file from the Tripwire Enterprise installation DVD to a temporary directory on the local drive:
   - **Command-line installer**: `te_agent/macOSX/te_agent.bin`
   - **GUI installer**: `te_agent/macOSX/te_agent.dmg`

   For a download installation, expand the download file to a directory on the local drive.
3. **For the command-line installer**, use the following command to launch the installer:
   ```bash
   ./te_agent.bin
   ```

   **For the GUI installer**, double-click on the `te_agent.dmg` file to open it, then double-click the `Tripwire Enterprise Agent.app` file.

   With either installation method, the software is installed to `/usr/local/tripwire/te/agent` and this location cannot be changed.
4. Follow the on-screen instructions to complete the installer.

**Note**  If you install the Event Generator, you can monitor the Agent system in real time. For more details, see *How Does an Event Generator Collect Audit Events?* in the *Tripwire Enterprise User Guide.*
5. If the TE Console you will use to manage this Agent uses a non-default HTTP port (the default port is 8080), you must edit the Agent's properties file to specify it:
   
a. On the Agent system, open `<te_root>/agent/data/config/agent.properties` in a text editor.
   
b. Add the following line, overwriting any existing `webserver.http.port` value:
   ```properties
   webserver.http.port=<Console_HTTP_port>
   ```
   
The Console's HTTP port is the value of the `webserver.http.port` property, specified in the `server.properties` file on the TE Console system.
   
c. Save the file.

6. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See Using Tag Files to Assign Tags to New TE Agents on page 72 for more information.

Follow these steps to create a tag file:

a. Create a text file named `agent.tags.conf` with the tags that you want to assign.

b. Copy the tag file to `<te_root>/agent/data/config` on the Agent system.

7. Start the Agent with the following command:
   ```bash
   launchctl start com.tripwire.te.agent
   ```

If you need to stop the Agent, use this command:
   ```bash
   launchctl stop com.tripwire.te.agent
   ```

Next For information on hardening your Tripwire Enterprise Agent installation, see the Tripwire Enterprise Hardening Guide, available for download from the Tripwire Customer Center.
To silently install Tripwire Enterprise Agent on an OS X system:

1. Log in to the system with root privileges.

2. For a DVD installation, copy the following file from the Tripwire Enterprise installation DVD to a temporary directory on the local drive:
   
   `te_agent/macosx/te_agent.bin`

   For a download installation, expand the download file to a directory on the local drive.

3. Use the following command to launch the installer:

   ```
   ./te_agent.bin --eula accept --silent --server-host <server_host> --server-port <server_port> --passphrase <services_password>
   ```

   For descriptions of command-line components, see Table 11 on the next page. The software is installed to `/usr/local/tripwire/te/agent` and this cannot be changed.

   By default, the installer also installs an Event Generator that uses port 1169 to communicate with Tripwire Enterprise Agent. To specify a different port, add:

   ```
   --install-rtm true --rtmport <EG_port>
   ```

4. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See Using Tag Files to Assign Tags to New TE Agents on page 72 for more information.

   Follow these steps to create a tag file:

   a. Create a text file named `agent.tags.conf` with the tags that you want to assign.

   b. Copy the tag file to `<te_root>/agent/data/config` on the Agent system.

5. Start the Agent with the following command:

   ```
   launchctl start com.tripwire.te.agent
   ```

   If you need to stop the Agent, use this command:

   ```
   launchctl stop com.tripwire.te.agent
   ```
Table 11. Command-line components for OS X silent installations

<table>
<thead>
<tr>
<th>Command-line Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--eula accept</td>
<td>Indicates your agreement with the Tripwire EULA.</td>
</tr>
<tr>
<td>--enable-fips</td>
<td>(Optional) Enables FIPS mode for the Agent.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For information on FIPS mode, see the Tripwire Enterprise Hardening Guide, available for download from the Tripwire Customer Center.</td>
</tr>
<tr>
<td>--http-port &lt;http_port&gt;</td>
<td>(Optional) If your TE Console is using a non-default HTTP port (8080 is the default), you must use this option to specify the HTTP port.</td>
</tr>
<tr>
<td>--install-rtm [true</td>
<td>false]</td>
</tr>
<tr>
<td>--passphrase &lt;services_password&gt;</td>
<td>The same Services Password entered when Tripwire Enterprise Console was installed.</td>
</tr>
<tr>
<td>--proxy-host &lt;proxy_host&gt;</td>
<td>(Optional) The hostname or IP address of a Tripwire Enterprise proxy.</td>
</tr>
<tr>
<td>--proxy-port &lt;proxy_port&gt;</td>
<td>(Optional) The number of the port on a Tripwire Enterprise proxy with which TE will communicate with the proxy. <strong>Note:</strong> For more information about proxies, see Configuring a Tripwire Enterprise Proxy for Agent Communication on page 117.</td>
</tr>
<tr>
<td>--rtmport &lt;EG_port&gt;</td>
<td>(Optional) If you enter a --install-rtm option, you can use this option to specify a non-default port for communications between the Event Generator and Tripwire Enterprise Agent. (The default port is 1169.)</td>
</tr>
<tr>
<td>--server-host &lt;server_host&gt;</td>
<td>The hostname or IP address of your Tripwire Enterprise Server.</td>
</tr>
<tr>
<td>--server-port &lt;server_port&gt;</td>
<td>The number of the services port on your Tripwire Enterprise Server (9898 by default). <strong>Note:</strong> You specified the services port when you installed Tripwire Enterprise Console software on your Tripwire Enterprise Server. The TE Server communicates with all TE Agents via the services port.</td>
</tr>
<tr>
<td>--tmp-dir &lt;installation_directory&gt;</td>
<td>(Optional) Specifies an alternative temporary directory for the installation.</td>
</tr>
</tbody>
</table>
Installing Tripwire Enterprise Agent on HP-UX

The HP-UX version of the Tripwire Enterprise Agent installer is a native SD-UX package (.depot) named te_agent.depot.

To install Tripwire Enterprise Agent on an HP-UX system, see:

- Interactive Installation for HP-UX (below)
- Silent Installation for HP-UX (on page 55)

Interactive Installation for HP-UX

To interactively install Tripwire Enterprise Agent on an HP-UX system:

1. Log in to the system with root privileges.

2. For a DVD installation, copy one of the following files from the Tripwire Enterprise installation DVD to a temporary directory on the local drive.
   - For Itanium IA-64: agent/hpux/ia64/te_agent.depot
   - For PA-RISC: agent/hpux/pa-risc/te_agent.depot

   For a download installation, expand the download file to a directory on the local drive.

3. To install the software in the default installation directory (/usr/local/tripwire/te/agent), launch the installer by entering the following command at a command prompt:

   `/usr/sbin/swinstall -s <depot_file_path>/te_agent.depot -x ask=true TWeagent`

   where <depot_file_path> is the absolute path to the depot file on your Tripwire Enterprise installation DVD (or in your download archive).

   To install the software in a different directory, replace TWeagent with the following value:

   `TWeagent:<installation_directory>/`

   **Note** If you install the software in a directory other than the default location, make a note of it. You will need the full path to start the Agent.

   The -x ask=true option is required in order to prompt the user for configuration options.

4. Follow the on-screen instructions to complete the installer.
5. If the TE Console you will use to manage this Agent uses a non-default HTTP port (the default port is 8080), you must edit the Agent's properties file to specify it:

   a. On the Agent system, open `<te_root>/agent/data/config/agent.properties` in a text editor.

   b. Add the following line, overwriting any existing `webserver.http.port` value:

   ```
   webserver.http.port=<Console_HTTP_port>
   ```

   The Console's HTTP port is the value of the `webserver.http.port` property, specified in the `server.properties` file on the TE Console system.

   c. Save the file.

6. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See *Using Tag Files to Assign Tags to New TE Agents on page 72* for more information.

   Follow these steps to create a tag file:

   a. Create a text file named `agent.tags.conf` with the tags that you want to assign.

   b. Copy the tag file to `<te_root>/agent/data/config` on the Agent system.

7. Start the Agent. For instructions, see *Managing the Tripwire Enterprise Agent Service on page 134*.

Next For information on hardening your Tripwire Enterprise Agent installation, see the *Tripwire Enterprise Hardening Guide*, available for download from the *Tripwire Customer Center*. 
Silent Installation for HP-UX

**Note** By installing Tripwire Enterprise Agent software, you consent to all terms and conditions outlined in the Tripwire EULA. For more information, see *The End-User License Agreement* on page 40.

To silently install Tripwire Enterprise Agent on an HP-UX system, complete the following tasks:

*Step 1. Converting the Depot File (below)*

*Step 2. Creating a Response File (below)*

*Step 3. Installing Tripwire Enterprise Agent (on the next page)*

**Step 1. Converting the Depot File**

To convert the depot package file (`te_agent.depot`) from “tape” format to a file system layout format:

1. Log in to the HP-UX system with root privileges.
2. At a command prompt, enter the following command:

   ```bash
   /usr/sbin/swcopy -s <depot_file_path>/te_agent.depot *
   ```

   where `<depot_file_path>` is the absolute path to the depot file on your Tripwire Enterprise installation DVD (or in your download archive).

**Step 2. Creating a Response File**

With an interactive installation, you provide answers to a series of questions presented by the Tripwire Enterprise Agent installer. With a silent installation on an HP-UX system, you enter your answers in a response file prior to installation. When you install the Agent (in *Step 3. Installing Tripwire Enterprise Agent on the next page*), the installer automatically gathers the required information from the response file.

This procedure creates a response file in the following location:

```
/var/spool/sw/catalog/TWeagent/TWeagent_FILES/response
```

To create a response file for silent installation of Tripwire Enterprise Agent on an HP-UX system:

1. Log in to the system with root privileges.
2. Enter the following `swask` command to generate the response file:

   ```bash
   /usr/sbin/swask -s /var/spool/sw TWeagent
   ```

3. Follow the on-screen instructions to complete the response file.
4. If the TE Console you will use to manage this Agent uses a non-default HTTP port (the default port is 8080), you must edit the response file to specify it:

   a. Open the te_agent.pkg file in a text editor.

   b. Add the following line:

   ```
   TE_SERVER_HTTP_PORT=<port>
   ```

   where `<port>` is the value of the `webserver.http.port` property, specified in the `server.properties` file on the TE Console system.

   c. Save the file.

**Step 3. Installing Tripwire Enterprise Agent**

To silently install Tripwire Enterprise Agent on an HP-UX system:

1. Log in to the system with root privileges.

2. To install the software in the default installation directory (`/usr/local/tripwire/te/agent`), enter the following `swinstall` command at a command prompt:

   ```
   /usr/sbin/swinstall -s /var/spool/sw TWeagent
   ```

   To install the software in a different directory, replace `TWeagent` with the following value:

   ```
   TWeagent:<installation_directory>/
   ```

   **Note** If you install the software in a directory other than the default location, make a note of it. You will need the full path to start the Agent.

3. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See *Using Tag Files to Assign Tags to New TE Agents* on page 72 for more information.

   Follow these steps to create a tag file:

   a. Create a text file named `agent.tags.conf` with the tags that you want to assign.

   b. Copy the tag file to `<te_root>/agent/data/config` on the Agent system.

4. Start the Agent. For instructions, see *Managing the Tripwire Enterprise Agent Service* on page 134.
Installing Tripwire Enterprise Agent on Linux

The Linux version of the TE Agent installer is a native RPM package. The native RPM package and usage license are embedded in the delivered binary file (te_agent.bin). To install TE Agent on a Linux system, see:

- *Interactive Installation for Linux* (below)
- *Silent Installation for Linux* (on page 59)

Interactive Installation for Linux

To interactively install Tripwire Enterprise Agent on a Linux system:

1. Log in to the system with root privileges.

2. For a DVD installation, copy the following file from the TE installation DVD to a temporary directory on the local drive:
   - For 32-bit: `te_agent/linux/i386/te_agent.bin`
   - For 64-bit: `te_agent/linux/x86_64/te_agent.bin`
   - For PPC: `te_agent/linux/ppc/te_agent.bin`

   For a download installation, expand the appropriate zip file (32-bit or 64-bit) to a temporary directory on the local drive.

3. To install the software in the default installation directory (`/usr/local/tripwire/te/agent`), launch the installer by entering the following command at a command prompt:

   ```bash
   ./te_agent.bin
   ```

   To install the software in a different directory, enter:

   ```bash
   ./te_agent.bin --install-dir <installation_directory>
   ```

   **Notes**
   You cannot specify a custom installation directory on Debian systems.
   
   If you install the software in a directory other than the default location, make a note of it. You will need the full path to start the Agent.
   
   If you install an Event Generator with the Agent, you can monitor the Agent system in real time. For more details, see *How Does an Event Generator Collect Audit Events?* in the *Tripwire Enterprise User Guide*.

4. Follow the on-screen instructions to complete the installer.
5. If the TE Console you will use to manage this Agent uses a non-default HTTP port (the default port is 8080), you must edit the Agent's properties file to specify it:

   a. On the Agent system, open `<te_root>/agent/data/config/agent.properties` in a text editor.

   b. Add the following line, overwriting any existing `webserver.http.port` value:

```
webserver.http.port=<Console_HTTP_port>
```

   The Console's HTTP port is the value of the `webserver.http.port` property, specified in the `server.properties` file on the TE Console system.

   c. Save the file.

6. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See *Using Tag Files to Assign Tags to New TE Agents* on page 72 for more information.

   Follow these steps to create a tag file:

   a. Create a text file named `agent.tags.conf` with the tags that you want to assign.

   b. Copy the tag file to `<te_root>/agent/data/config` on the Agent system.

7. Start the Agent. For instructions, see *Managing the Tripwire Enterprise Agent Service* on page 134.

| Next | For information on hardening your Tripwire Enterprise Agent installation, see the *Tripwire Enterprise Hardening Guide*, available for download from the Tripwire Customer Center. |
Silent Installation for Linux

Note  By installing Tripwire Enterprise Agent software, you consent to all terms and conditions outlined in the Tripwire EULA. For more information, see The End-User License Agreement on page 40.

To silently install Tripwire Enterprise Agent on a Linux system:

1. Log in to the system with root privileges.

2. For a DVD installation, copy the following file from the Tripwire Enterprise installation DVD to a temporary directory on the local drive:
   - For 32 bit: te_agent/linux/i386/te_agent.bin
   - For 64 bit: te_agent/linux/x86_64/te_agent.bin
   - For PPC: te_agent/linux/ppc/te_agent.bin

   For a download installation, expand the download file to a directory on the local drive.

3. To install the software in the default installation directory (/usr/local/tripwire/te/agent), launch the installer by entering the following command at a command prompt:
   
   ./te_agent.bin --eula accept --silent --server-host <server_host> --server-port <server_port> --passphrase <services_password>

   To install the software in a different directory, add the following option:

   --install-dir <installation_directory>

   By default, the installer also installs an Event Generator that uses port 1169 to communicate with Tripwire Enterprise Agent. To specify a different port, add the following options:

   --install-rtm true --rtmport <EG_port>

   For descriptions of command-line components, see Table 12 on the next page.

   Note  If you install the software in a directory other than the default location, make a note of it. You will need the full path to start the Agent.

4. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See Using Tag Files to Assign Tags to New TE Agents on page 72 for more information.

   Follow these steps to create a tag file:

   a. Create a text file named agent.tags.conf with the tags that you want to assign.
   b. Copy the tag file to <te_root>/agent/data/config on the Agent system.

5. Start the Agent. For instructions, see Managing the Tripwire Enterprise Agent Service on page 134.
<table>
<thead>
<tr>
<th>Command-line Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--eula accept</td>
<td>Indicates your agreement with the Tripwire EULA.</td>
</tr>
<tr>
<td>--enable-fips</td>
<td>(Optional) Enables FIPS mode for the Agent. <strong>Note:</strong> For information on FIPS mode, see the <em>Tripwire Enterprise Hardening Guide</em>, available for download from the <em>Tripwire Customer Center</em>.</td>
</tr>
<tr>
<td>--http-port &lt;http_port&gt;</td>
<td>(Optional) If your TE Console is using a non-default HTTP port (8080 is the default), you must use this option to specify the HTTP port.</td>
</tr>
<tr>
<td>--install-dir &lt;installation_directory&gt;</td>
<td>(Optional) The full path to a non-default installation directory.</td>
</tr>
<tr>
<td>--install-rtm [true</td>
<td>false]</td>
</tr>
<tr>
<td>--passphrase &lt;services_password&gt;</td>
<td>The same Services Password entered when Tripwire Enterprise Console was installed.</td>
</tr>
<tr>
<td>--proxy-host &lt;proxy_host&gt;</td>
<td>(Optional) The hostname or IP address of a Tripwire Enterprise proxy.</td>
</tr>
<tr>
<td>--proxy-port &lt;proxy_port&gt;</td>
<td>(Optional) The number of the port on a Tripwire Enterprise proxy with which TE will communicate with the proxy. <strong>Note:</strong> For more information about proxies, see <em>Configuring a Tripwire Enterprise Proxy for Agent Communication on page 117</em>.</td>
</tr>
<tr>
<td>--rtmport &lt;EG_port&gt;</td>
<td>(Optional) If you enter a --install-rtm option, you can use this option to specify a non-default port for communications between the Event Generator and Tripwire Enterprise Agent. (The default port is 1169.)</td>
</tr>
<tr>
<td>--server-host &lt;server_host&gt;</td>
<td>The hostname or IP address of your Tripwire Enterprise Server.</td>
</tr>
<tr>
<td>--server-port &lt;server_port&gt;</td>
<td>The number of the services port on your Tripwire Enterprise Server (9898 by default). <strong>Note:</strong> You specified the services port when you installed Tripwire Enterprise Console software on your Tripwire Enterprise Server. The TE Server communicates with all TE Agents via the services port.</td>
</tr>
<tr>
<td>--tmp-dir &lt;installation_directory&gt;</td>
<td>(Optional) Specifies an alternative temporary directory for the installation.</td>
</tr>
</tbody>
</table>
Installing Tripwire Enterprise Agent on Solaris

The Solaris version of the Tripwire Enterprise Agent installer is a native Solaris package. The package and usage license are embedded in the package file (te_agent.pkg).

To install Tripwire Enterprise Agent on a Solaris system, see:

- *Interactive Installation for Solaris* (below)
- *Silent Installation for Solaris* (on page 64)

Interactive Installation for Solaris

To interactively install Tripwire Enterprise Agent on a Solaris system:

1. Log in to the system with root privileges or a local, non-root user account that has been assigned the Software Installation profile with the following command:

   ```
   usermod -P "Software Installation" <username>
   ```

   **Tip** To grant a non-root user account the ability to access files and directories that would otherwise be unreadable, add the following command:

   ```
   usermod -K defaultpriv=basic,file_dac_read, file_dac_search <username>
   ```

   Where `<username>` is the name of the user account. For more information about Solaris Role-Based Access Controls, see the `rbac(5)` and `privileges(5)` Solaris man pages.

2. For a DVD installation, copy one of the following files from the Tripwire Enterprise installation DVD to a temporary directory on the local drive.

   - For SPARC: `te_agent/solaris/sparcv9/te_agent.pkg`
   - For 64-bit: `te_agent/solaris/amd64/te_agent.pkg`

   For a download installation, expand the download file to a temporary directory on the local drive.

3. Launch the installer with one of the following commands.

   If you logged in with root privileges, enter:

   ```
   pkgadd -d <pkg_file_path>/te_agent.pkg TWeagent
   ```

   If you logged in with a local user account, enter:

   ```
   /usr/bin/pfexec /usr/sbin/pkgadd -d <pkg_file_path> TWeagent
   ```

   where `<pkg_file_path>` is the path to the temporary directory.

4. Follow the on-screen instructions to complete the installer.
5. If the TE Console you will use to manage this Agent uses a non-default HTTP port (the default port is 8080), you must edit the Agent's properties file to specify it:
   a. On the Agent system, open <te_root>/agent/data/config/agent.properties in a text editor.
   b. Add the following line, overwriting any existing webserver.http.port value:
      
      webserver.http.port=<Console_HTTP_port>
      
      The Console's HTTP port is the value of the webserver.http.port property, specified in the server.properties file on the TE Console system.
   c. Save the file.

6. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See Using Tag Files to Assign Tags to New TE Agents on page 72 for more information.
   
   Follow these steps to create a tag file:
   a. Create a text file named agent.tags.conf with the tags that you want to assign.
   b. Copy the tag file to <te_root>/agent/data/config on the Agent system.

7. Start the Agent. For instructions, see Managing the Tripwire Enterprise Agent Service on page 134.

8. If the Agent will use a TE Event Generator for real-time monitoring in a non-global zone, complete the steps in Configuring the Global Event Source for Non-Global Zones (on the next page).

Next For information on hardening your Tripwire Enterprise Agent installation, see the Tripwire Enterprise Hardening Guide, available for download from the Tripwire Customer Center.
Configuring the Global Event Source for Non-Global Zones

When you install TE Agent on a Solaris system's global zone, the Global Event Source is included with the installation. If you want to run the TE Event Generator on a Solaris system, you must configure the Global Event Source on the system's global zone. The Global Event Source gathers operating system events and makes them available to the Event Generator. In turn, the Event Generator forwards the events to the Agent.

On a Solaris 10 system, the SUNWzoner and SUNWzoneu packages are required to run the TE Event Generator. If you are using the Solaris Live Update feature, you may also want to install the SUNW1uzone package.

To enable the Global Event Source once TE Agent has been installed on a Solaris system, run the following command on the system's global zone:

```
svcadm enable teges
```

To configure the Global Event Source, complete these steps for each non-global zone:

1. In the zonecfg file, edit the zone's configuration: zonecfg -z <zone_name>

2. Run one of the following sets of commands:

   **Solaris 10:**
   ```
   add fs
   set dir=/var/tripwire/doors
   set special=/var/tripwire/doors
   set type=lofs
   end
   commit
   exit
   ```

   **Solaris 11:**
   ```
   add fs
   set dir=/opt/tripwire/doors
   set special=/opt/tripwire/doors
   set type=lofs
   end
   commit
   exit
   ```

3. To reboot the zone, run `zlogin <zone_name> reboot`

   **To create and mount an LOFS directory (without rebooting), run:**

   **Solaris 10:**
   ```
   mkdir -p <zone_path>/root/var/tripwire/doors
   mount -F lofs /var/tripwire/doors <zone_path>/root/var/tripwire/doors
   ```

   **Solaris 11:**
   ```
   mkdir -p <zone_path>/root/opt/tripwire/doors
   mount -F lofs /opt/tripwire/doors <zone_path>/root/opt/tripwire/doors
   ```


Silent Installation for Solaris

**Note** By installing Tripwire Enterprise Agent software, you consent to all terms and conditions outlined in the Tripwire EULA. For more information, see *The End-User License Agreement on page 40.*

To silently install Tripwire Enterprise Agent on a Solaris system, complete the following tasks:

*Step 1. Creating a Response File (below)*

*Step 2. Creating an Admin File (on the next page)*

*Step 3. Adding the Package File (on page 66)*

**Step 1. Creating a Response File**

With an interactive installation, you provide answers to a series of questions presented by the Tripwire Enterprise Agent installer. With a silent installation on a Solaris system, you enter your answers in a response file prior to installation. When you install the Agent (in *Step 3. Adding the Package File on page 66*), the installer automatically gathers the required information from the response file.

To create a response file for a Solaris system:

1. Log in to the system with root privileges or a local, non-root user account that has been assigned the Software Installation profile.

   ```bash
   usermod -P "Software Installation" <username>
   ```

   **Tip** To assign root-level, file-read privileges to a local, non-root user account, log in with root privileges and run the following command:

   ```bash
   usermod -K defaultpriv=basic,file_dac_read,
   file_dac_search <username>
   ```

   Where `<username>` is the name of the local user account. For more information, see the `usermod(1M)` and `pfexec(1)` Solaris man pages.

2. For a DVD installation, copy one of the following files from the Tripwire Enterprise installation DVD to a temporary directory on the local drive.

   - For SPARC: `te_agent/solaris/sparcv9/te_agent.pkg`
   - For 64-bit: `te_agent/solaris/amd64/te_agent.pkg`

   For a download installation, expand the download file to a temporary directory on the local drive.
3. Launch the installer with one of the following commands.

If you logged in with root privileges, enter:

```
pkgask -d <pkg_file_path>/te_agent.pkg
-r <response_file_path>/response_file TWeagent
```

If you logged in with a local user account, enter:

```
/usr/bin/pfexec /usr/sbin/pkgask -d <pkg_file_path>/te_agent.pkg
-r <response_file_path>/response_file TWeagent
```

For command-line component definitions, see Table 13.

4. Follow the on-screen instructions to complete the installer.

5. If the TE Console you will use to manage this Agent uses a non-default HTTP port (the default port is 8080), you must edit the response file to specify it:

a. Open the te_agent.pkg file in a text editor.

b. Add the following line:

```
TE_SERVER_HTTP_PORT='<port>
```

where <port> is the value of the webserver.http.port property, specified in the server.properties file on the TE Console system.

c. Save the file.

6. If the Agent will use a TE Event Generator for real-time monitoring in a non-global zone, complete the steps in *Configuring the Global Event Source for Non-Global Zones* on page 63.

### Table 13. Command-line components for the Solaris response file

<table>
<thead>
<tr>
<th>Command-line Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d &lt;pkg_file_path&gt;</td>
<td>The full path name of the directory to which you copied the Solaris package file (te_agent.pkg).</td>
</tr>
<tr>
<td>-r &lt;response_file_path&gt;</td>
<td>The full path name of the directory in which the response file (response_file) will be created.</td>
</tr>
</tbody>
</table>

### Step 2. Creating an Admin File

An **admin file** defines how the pkgadd utility installs packages on a Solaris system. To silently install Tripwire Enterprise Agent on a Solaris system, you must create a customized copy of the system’s default admin file.

**To create a customized admin file:**

1. Locate the following default admin file:

```
/var/sadm/install/admin/default
```
2. Copy the default admin file to another local directory. Name the new file admin_file.

3. Edit admin_file to match the following content:

```plaintext
#ident "@(#)default 1.4 92/12/23 SMI" /* SVr4.0 1.5.2.1 */
mail=
instance=overwrite
partial=ask
runlevel=ask
idepend=ask
rdepend=ask
space=ask
setuid=ask
conflict=ask
action=nocheck
basedir=default
```

**Step 3. Adding the Package File**

1. To add the Solaris package file (te_agent.pkg), enter one of the following commands at a command prompt on the Solaris system.

   **If you created the response file with root privileges** (see Step 1. Creating a Response File on page 64), enter:

   `pkgadd -n -r <response_file_path>/response_file
   -a <admin_file_path>/admin_file -d <pkg_file_path>/te_agent.pkg TWeagent`

   **If you created the response file with a local user account**, enter:

   `/usr/bin/pfexec /usr/sbin/pkgadd -d <pkg_file_path>/te_agent.pkg
   -r <response_file_path>/response_file TWeagent`

   For command-line component definitions, see Table 14 (below).

2. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See Using Tag Files to Assign Tags to New TE Agents on page 72 for more information. To create a tag file:

   a. Create a text file named agent.tags.conf with the tags that you want to assign.

   b. Copy the tag file to <te_root>/agent/data/config on the Agent system.

3. Start the Agent. For instructions, see Managing the Tripwire Enterprise Agent Service on page 134.

**Table 14. Command-line components for the Solaris package file**

<table>
<thead>
<tr>
<th>Command-line Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a &lt;admin_file_path&gt;</td>
<td>The full path to the admin file (admin_file).</td>
</tr>
<tr>
<td>-d &lt;pkg_file_path&gt;</td>
<td>The full path to the package file (te_agent.pkg).</td>
</tr>
<tr>
<td>-r &lt;response_file_path&gt;</td>
<td>The full path to the response file (response_file).</td>
</tr>
</tbody>
</table>
Installing Tripwire Enterprise Agent on Windows

The Windows Tripwire Enterprise Agent installer uses Microsoft Windows Installer (.msi) technology to implement a native installer package, a single file package named te_agent.msi.

To install Tripwire Enterprise Agent on a Windows system, see:

- Interactive Installation for Windows (below)
- Silent Installation for Windows (on page 69)

Interactive Installation for Windows

To interactively install Tripwire Enterprise Agent on a Windows system:

1. Log in to the system with Administrator privileges.

2. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See Using Tag Files to Assign Tags to New TE Agents on page 72 for more information. To create a tag file:
   a. On the Agent system, create a directory at:
      
      C:\Program Files\Tripwire\TE\Agent\data\config
      
      or at an equivalent location if you are installing TE Agent to a non-default location.
   b. Create a text file named agent.tags.conf in this directory with the tags that you want to assign.

3. For a DVD installation, navigate to the appropriate directory for your platform:

   For 32-bit: \te_agent\windows\i386
   For 64-bit: \te_agent\windows\x86_64

   For a download installation, expand the appropriate zip file (32-bit or 64-bit) to a temporary directory on the local drive.

4. Launch the installer by executing the te_agent.msi file.

   Follow the on-screen instructions to complete the installer.

   **Note** If you install the Event Generator, you can monitor the Agent system in real time. For more details, see How Does an Event Generator Collect Audit Events? in the Tripwire Enterprise User Guide.
5. If the TE Console you will use to manage this Agent uses a non-default HTTP port (the default port is 8080), you must edit the Agent's properties file to specify it:

   a. Stop the TE Agent service:
   
      <te_root>\Agent\bin\twdaemon stop
   
   a. On the Agent system, open <te_root>\Agent\data\config\agent.properties in a text editor.
   
   b. Add the following line, overwriting any existing webserver.http.port value:

      webserver.http.port=<Console_HTTP_port>

      The Console's HTTP port is the value of the webserver.http.port property, specified in the server.properties file on the TE Console system.
   
   c. Save the file, then start the TE Agent service

      <te_root>\Agent\bin\twdaemon start

6. If you haven't already, start the Agent as described in Managing the Tripwire Enterprise Agent Service on page 134.

Next For information on hardening your Tripwire Enterprise Agent installation, see the Tripwire Enterprise Hardening Guide, available for download from the Tripwire Customer Center.
Silent Installation for Windows

**Note** By installing Tripwire Enterprise Agent software, you consent to all terms and conditions outlined in the Tripwire EULA. For more information, see *The End-User License Agreement* on page 40.

To silently install Tripwire Enterprise Agent on a Windows system:

1. (Optional) If you create a tag file for this Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See *Using Tag Files to Assign Tags to New TE Agents* on page 72 for more information.

   The tag file must be present before the Agent starts for the first time. If you want the installer to start the Agent after installation (the default behavior), you must create the tag file before running the installer:

   a. On the Agent system, log in with Administrator privileges and create a directory at
      
      `C:\Program Files\Tripwire\TE\Agent\data\config`

      or at an equivalent location if you are installing TE Agent to a non-default location.

   b. Create a text file named `agent.tags.conf` in this directory with the tags that you want to assign.

   **Note** If you plan to start the Agent manually after installation and set `START_AGENT=false` in step 2, you can create the tag file as described above after running the installer.

2. Run the following command on the Agent's command line:

   ```
   te_agent.msi /qn TE_SERVER_HOSTNAME=<server_host>
   TE_SERVER_PORT=<server_port> SERVICES_PASSWORD=<services_password>
   START_AGENT=[true|false] INSTALLDIR=<install_path> INSTALL_RTM=[true|false]
   RTMPORT=<Event_Generator_port> ACCEPT_EULA=[true|false]
   ```

   For command-line component definitions, see *Table 15 on the next page*.

   **Notes** All command-line components are case sensitive.

   The `TE_SERVER_PORT`, `START_AGENT`, `INSTALLDIR`, and `INSTALL_RTM` parameters are optional since they have default values. Otherwise, all of the options are required in order to have a functional installation.
### Table 15. Command-line components for Windows silent installations

<table>
<thead>
<tr>
<th>Command-line Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCEPT_EULA= [true</td>
<td>false]</td>
</tr>
<tr>
<td>INSTALLDIR= &lt;install_path&gt;</td>
<td>(Optional) By default, the command installs the software to: C:\Program Files\Tripwire\TE\Agent\ To install Tripwire Enterprise Agent in a non-default directory, enter this option with the full path to the directory. <strong>Note:</strong> If you install the software in a directory other than the default location, make a note of it. You will need the full path to start the Agent.</td>
</tr>
<tr>
<td>INSTALL_FIPS= [true</td>
<td>false]</td>
</tr>
<tr>
<td>INSTALL_RTM= [true</td>
<td>false]</td>
</tr>
<tr>
<td>RTMPORT= &lt;Event_Generator_port&gt;</td>
<td>(Optional) If you install an Event Generator (EG) with the INSTALL_RTM command, the EG communicates with the Agent via port 1169 by default. To use a different port, enter the port number here.</td>
</tr>
<tr>
<td>SERVICES_PASSWORD= &lt;services_password&gt;</td>
<td>The same Services Password entered when Tripwire Enterprise Console was installed.</td>
</tr>
<tr>
<td>START_AGENT= [true</td>
<td>false]</td>
</tr>
<tr>
<td>TE_PROXY_HOSTNAME= &lt;te_proxy_hostname&gt;</td>
<td>(Optional) The hostname or IP address of a Tripwire Enterprise proxy.</td>
</tr>
<tr>
<td>TE_PROXY_PORT= &lt;te_proxy_port&gt;</td>
<td>(Optional) The number of the port on a Tripwire Enterprise proxy with which TE will communicate with the proxy. <strong>Note:</strong> For more information about proxies, see Configuring a Tripwire Enterprise Proxy for Agent Communication on page 117.</td>
</tr>
<tr>
<td>TE_SERVER_HOSTNAME= &lt;server_host&gt;</td>
<td>The hostname or IP address of your Tripwire Enterprise Server.</td>
</tr>
<tr>
<td>TE_SERVER_HTTP_PORT= &lt;http_port&gt;</td>
<td>(Optional) If your TE Console is using a non-default HTTP port (8080 is the default), you must use this option to specify the HTTP port.</td>
</tr>
<tr>
<td>Command-line Component</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>TE_SERVER_HTTPS_PORT= &lt;https_port&gt;</td>
<td>(Optional) If you are using a non-default HTTPS port on your TE Server (8080 is the default port), you must use this option to specify the HTTPS port.</td>
</tr>
</tbody>
</table>
| TE_SERVER_PORT= <server_port> | (Optional) The number of the services port on your Tripwire Enterprise Server (9898 by default).  
**Note:** You specified the services port when you installed Tripwire Enterprise Console. The Tripwire Enterprise Server communicates with all TE Agents via the services port. |
Using Tag Files to Assign Tags to New TE Agents

Tag files can be deployed with new TE Agent installations to simplify onboarding of new systems. A tag file is a text file on an Agent system that specifies tags to be assigned to the asset the first time it is added to a TE Console.

Tag files can be useful when automatic tagging profiles alone are not sufficient to tag assets, for example in cases when different assets share the same IP address or hostname.

| Notes | For more information on tags, tagging profiles, and how they can be used in TE, see Getting Started with Tags in the Tripwire Enterprise User Guide. While tag files work the same way on TE Agents and Axon Agents, the implementation and file formats are slightly different. For information on using tag files with Axon Agents, see Using Tag Files to Assign Tags to New Axon Agents on page 96. |

Consider the following points when using tag files:

- Specific instructions for deploying tag files on each platform are in the TE Agent installation procedures in Chapter 2: Installing Tripwire Enterprise Agent (on page 39).

- Tag files must be named agent.tags.conf, and must be located in the Agent system's <te_root>/agent/data/config directory. The format for a tag file is specified in Tag File Format for TE Agents (on the next page).

- A tag file must be present before the Agent has started for the first time, and the tags in the file are only assigned the first time the asset is added to a TE Console. Subsequent restarts will not add tags or modify the tags already assigned.

- Tags in a tag file are added in addition to the system tags (Operating System, Status, etc.) that are automatically assigned when an asset is added to TE Console.

- Tags and tag sets used in the tag file must already exist within a TE Console when the asset is added. If new tags or tag sets are included in a tag file, no tags in the file will be assigned, and the Console will generate an error.

- Only user-created tags and tag sets can be added using a tag file. If system tag sets or operational tag sets are included in a tag file, they will be ignored.

- If an asset's tag file contains errors when it is added to TE Console, the asset is tagged with a Health:Uncategorized Error tag. In addition, an error message with the category Asset View Change will be added to the Log Manager and tserver.log file.
**Tag File Format for TE Agents**

One tag set and tag name are allowed per line of the tag file, using the following format:

```plaintext
<tag_set_name>:<tag>
```

For example:

```plaintext
Purpose:Application
Importance:Critical
Policy:CIS
```

Comments can be included in the tag file if they are preceded by a `#` character. For example:

```plaintext
# Comment about the file
Purpose:Application
Importance:Critical
Policy:CIS
```

Special characters can be used in tag sets and tag names, but the `:` and `#` characters must be escaped with the `\` character if they are used. White space will be ignored in the tag set and tag declaration. For example:

```plaintext
# White Space
Purpose: Application
# Hash Tag
\#HashtagSet:Hash\#Tag
# Colon
\:ColonSet:Colon\:Tag
```
Configuring TLS Versions for Tripwire Enterprise Agent

In Tripwire Enterprise 8.4.1 and later, you can specify the versions of TLS that are used to secure communication between the TE Console and TE Agents. To configure the TLS version used, you must edit the Console properties file, and also the Agent properties file on each TE Agent system.

Notes  To specify the TLS version used by Axon Agents, see Configuring TLS Versions for Axon Agent on page 103.

An embedded TE Agent is installed on each TE Console system, and the TLS version for this Agent must be configured like any other.

To configure TLS versions for TE Console and TE Agents (version 8.4.1 and later):

1. Make sure that all TE Agents are upgraded to version 8.4.1 or later (or 8.4.0 for AIX and Linux PPC Agents).
   
   The versions of TLS that are supported on a TE Agent depend on the JRE that is installed with that Agent. TE Agent 8.4.0 and later uses Oracle Java 8 for almost all platforms, except for AIX, HPUX, and Linux PPC.

2. Configure TE Console to temporarily accept connections using all versions of TLS:
   a. On the TE Console system, open the Console properties file in a text editor:
      <te_root>/server/data/config/server.properties
   b. Add the following lines to the file:
      tw.rmi.clientProtocols=TLSv1,TLSv1.1,TLSv1.2
      tw.rmi.serverProtocols=TLSv1,TLSv1.1,TLSv1.2,SSlv2Hello
   c. Save the server.properties file.
   d. Restart the TE Console service:
      <te_root>/server/bin/twservices restart

Notes  SSlv2Hello is required in the tw.rmi.serverProtocols property for TE Consoles that are not running in FIPS mode, but this protocol is only used for initial Console to Agent registration, not to secure subsequent communication.

For TE Consoles running in FIPS mode, omit SSlv2Hello from the tw.rmi.serverProtocols property.
3. **On each** TE Agent system where you want to specify the TLS version:

   a. Open the TE Agent properties file in a text editor:

   `<te_root>/agent/data/config/agent.properties`

   b. Add the `tw.rmi.clientProtocols` and `tw.rmi.serverProtocols` properties from step 2b, specifying **only** the TLS versions that you want this TE Agent to use. For example, to restrict the Agent to only connect using TLS 1.2, add:

   ```
   tw.rmi.clientProtocols=TLSv1.2
   tw.rmi.serverProtocols=TLSv1.2
   ```

   To configure the Agent to connect using multiple TLS versions, add:

   ```
   tw.rmi.clientProtocols=TLSv1.2,TLSv1.1
   tw.rmi.serverProtocols=TLSv1.2,TLSv1.1
   ```

   **Note** Make a note of all TLS versions that you specify for Agents. You will need this information in the next step.

   c. Save the `agent.properties` file.

   d. Restart the TE Agent service as described in *Managing the Tripwire Enterprise Agent Service* on page 134.

4. In TE Console, verify that all TE Agents are still communicating with the Console.

   If any Agents cannot connect, you may need to repeat the previous step to specify a different version of TLS that is supported on that Agent system.

5. Now, configure the TE Console system to restrict the TLS versions:

   a. Open the Console properties file in a text editor:

   `<te_root>/server/data/config/server.properties`

   b. Edit `tw.rmi.clientProtocols` and `tw.rmi.serverProtocols` to remove any TLS versions that aren't required to communicate with the Agents you configured in step 3.

   **Note** If you have AIX or Linux PPC Agents, you must include TLSv1 for both properties, since this is the most recent version that these platforms support.

   c. Save the `server.properties` file.

   d. Restart the TE Console service:

   `<te_root>/server/bin/twservices restart`

6. Use NMAP or a similar utility to verify that the correct version of TLS is being used to secure communication between TE Console and each TE Agent.
Upgrading Tripwire Enterprise Agent

To upgrade a Tripwire Enterprise Agent, complete the following steps:

*Step 1. Install Agent Update Packs (on the next page)*

*Step 2. Upgrade Tripwire Enterprise Agent Software (on page 78)*

During an upgrade, Tripwire Enterprise will install either the 32-bit or 64-bit TE Agent software, matched to the operating system of the Agent system. If you want to upgrade 32-bit TE Agent software on a 64-bit operating system, you must manually uninstall and re-install the TE Agent software.

**Note**
You cannot use this procedure to upgrade TE Agent on a platform that is not supported by the current version of Tripwire Enterprise. For a complete list of supported platforms for the current TE release, see http://www.tripwire.com/register/tripwire-enterprise-platform-and-device-support.

Axon Agent software cannot be upgraded from the TE Console. For Axon Agent upgrade instructions, see Upgrading Axon Agent on page 98.

If you upgrade a TE Agent running a platform that supports Event Generators (see Supported Platforms on page 43), Tripwire Enterprise also:

1. Installs an Event Generator on the Agent system,
2. Enables audit-event collection and real-time monitoring (RTM) for the Agent, and
3. Specifies port 1169 (TCP) as the port on the Agent system to be used by Tripwire Enterprise for all communications with the Event Generator.

You can override this default behavior for Linux and Windows TE Agents by uploading a properties file (in the procedure below) containing one or both of the following lines:

```
install_rtm=false
rtm_port=<port_number>
```

where:

- `install_rtm=false` prevents the installation of Event Generators, and
- `<port_number>` specifies a port other than 1169.

**Notes**
When upgrading TE Agent on a Solaris 10 system, the `install_rtm` option cannot be used to prevent the installation of an Event Generator. An Event Generator is always installed.

When upgrading TE Agent on an AIX system, Tripwire does **not** recommend setting the `install_rtm` flag to `false` in the properties file, even if you do not intend to use real-time monitoring or Event Generator functionality with the Agent. If you do not want to use real-time monitoring, shut down the Event Generator (stopsrc –s teeg) after upgrading the Agent.
Step 1. Install Agent Update Packs

To upgrade Tripwire Enterprise Agent, you must first install Agent update packs on your Tripwire Enterprise Server.

**To install Agent update packs on a UNIX or Linux TE Server:**

1. Log in to your TE Server as a privileged user.
2. To create a local directory for the Agent update packs, use these commands:
   
   ```sh
   mkdir <te_root>/server/lib/updaters
   chown tripwire:tripwire <te_root>/server/lib/updaters
   ```

3. To copy the Agent update pack directory from your Tripwire Enterprise installation DVD (or Web download) to the Tripwire Enterprise Console installation directory, enter:
   
   ```sh
   cp -r updaters/* <te_root>/server/lib/updaters
   ```

   **Note** Do not unzip the files. The installer will unzip the files automatically at a later point.

4. To change directories to the Agent update pack directory, enter:
   
   ```sh
   cd <te_root>/server/lib/updaters
   ```

5. To configure the user permissions for all contents of the Agent update pack directory, enter:
   
   ```sh
   chmod 0444 *
   chown tripwire:tripwire *
   ```

**To install Agent update packs on a Windows TE Server:**

1. Create the following directory:
   
   ```sh
   <te_root>\Server\lib\updaters
   ```

2. Copy all zip files from the Agent update pack directory (updaters) on your Tripwire Enterprise installation DVD (or Web download) to the new `updaters` directory on the TE Server.

   **Note** Do not unzip the files. The installer will unzip the files automatically at a later point.

3. To configure the user permissions for the `updaters` directory on the TE Server:
   
   a. In Windows Explorer, right-click the directory and select **Properties**.

   b. In the Properties dialog, clear (disable) the **read-only** attribute and verify that the Administrators user group has the **Full Control** permission.
Step 2. Upgrade Tripwire Enterprise Agent Software

Notes  When upgrading a TE Agent on a Solaris system, the procedure in this section does not allow you to change the user account with which the Agent is running. For more information, see Installing Tripwire Enterprise Agent on Solaris on page 61.

To upgrade a TE Agent on a Solaris system, the upgrade must run as the root user, and root must be added as an authorized user to the at.allow file. If you edit this file, you may need to create a policy waiver for some Tripwire-published policies.

To upgrade Tripwire Enterprise Agent software on one or more Agent systems:

1. In the Manager bar of TE Console, click NODES.
2. In the tree pane, select the node group that contains the TE Agent nodes for the systems to be upgraded.
3. To upgrade specific TE Agents, select the check box of each Agent node (or node group) in the main pane.

   To upgrade all TE Agents displayed in the selected node group, do not select any check boxes.
4. Click Modify > Upgrade.
5. In the Upgrade Agents dialog, click Next.
6. (Optional) To upload a properties file:
   a. Click Select.
   b. Click Browse.
   c. In the Choose File dialog, select the file and click Open.
   d. Click Upload.
7. Click Finish.

Tip  If an error occurs, Tripwire Enterprise will generate an Error message in the Log Manager. To begin troubleshooting, review the Error message.

8. For AIX systems only, perform the following steps to enable real-time and Event Generator functionality:
   a. Log into the AIX box with root privileges.
   b. Run <te root>/sup/rtm/teauditconfig.
   c. Start GES (startsrc -s teges).
Uninstalling Tripwire Enterprise Agent

Caution

The TE Console software can only be upgraded if TE Agent is installed on the TE Console system. For this reason, Tripwire strongly recommends that you **not** uninstall TE Agent on the system where TE Console is installed.

To uninstall Tripwire Enterprise Agent:

1. Log in to the system with root or Administrator privileges.
2. At a command prompt, enter the appropriate command.

   **UNIX and OS X:** `<te_root>/agent/bin/uninstall.sh [--removeall] [--force]`

   **Windows:** `<te_root>\Agent\bin\uninstall.cmd [--removeall] [--force]`

   For descriptions of command options, see Table 16.

   **Note**
   On a Windows system, Tripwire Enterprise can also be removed with the Add/Remove Programs feature in the Control Panel.

3. **For AIX systems only,** restore the AIX audit configuration files. For more information, see *Restoring Audit Configuration Files on page 48.*

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--force</strong></td>
<td>If you enter the <strong>--removeall</strong> option, this option removes the files and directories without presenting any confirmation prompts.</td>
</tr>
<tr>
<td><strong>--removeall</strong></td>
<td>Removes all files and directories contained in the Tripwire Enterprise installation directory (<code>&lt;te_root&gt;</code>). If you omit this option from the command, the uninstaller will retain some of the installation directory's contents, including some Tripwire Enterprise configuration files and temporary data.</td>
</tr>
</tbody>
</table>
Chapter 3.
Installing Tripwire Axon Agent
Getting Started with Tripwire Axon Agent

**Tripwire Axon Agent** is Tripwire’s new generation of agent technology. The Axon Agent is installed on an endpoint to be monitored, and provides data to Tripwire Enterprise Console.

The **Axon Bridge** is a component through which Axon Agents deliver data to a Tripwire Enterprise Server. To connect with Agents, the Axon Bridge on a Tripwire Enterprise Server uses the Transport Layer Security (TLS) protocol. Therefore, each Axon Agent needs a set of X.509 certificates in order to communicate with the Axon Bridge.

To acquire these certificates, you must create a pre-shared key that is used to authenticate a newly-connected Axon Agent while it obtains a certificate to use for subsequent connections. The first time that an Axon Agent attempts to connect with the Axon Bridge, they complete the following steps:

1. The Axon Agent establishes an anonymous TLS connection with the Axon Bridge.
2. The Agent sends an X.509 Certificate Signing Request (CSR) to the Bridge. If the Agent has a registration pre-shared-key file, the pre-shared key is included in the request.
3. The Axon Bridge verifies the CSR and pre-shared key, and it sends the Agent a set of signed X.509 certificates.
4. The Agent reads the response and locally stores copies of 1) the Axon Bridge Certificate Authority (CA), and 2) the signed certificates.
5. The Agent disconnects from the Axon Bridge and deletes its `registration_pre_shared_key.txt` file.
6. With the signed certificates, the Agent reconnects with the Axon Bridge and establishes a secure TLS session.

**Supported Platforms**

For a current list of platforms that support Axon Agent, see:

http://www.tripwire.com/register/tripwire-axon-platform-support
Required Ports and Protocols

The tables in this section list the services installed with Tripwire Enterprise Console, and the default ports used. Figure 11 below illustrates these connections.

Table 17. Bridge services installed with Tripwire Enterprise Console

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Listening Ports</th>
<th>Requires Firewall Access?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>twservices</td>
<td>5670</td>
<td>Y</td>
<td>The Axon Agent's connection port to the Axon Bridge.</td>
</tr>
</tbody>
</table>

Table 18. Required ports for the Bridge service on a Tripwire Enterprise Server

<table>
<thead>
<tr>
<th>Default Port/Protocol</th>
<th>Configurable During Installation?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5670/TCP/TLS</td>
<td>No</td>
<td>Used for inbound communication received from Axon Agents.</td>
</tr>
</tbody>
</table>

Figure 11. Axon Agent ports and protocols

Note: All communication conducted via TCP, unless otherwise noted.
Installing Axon Agent

This section describes the process to install and configure Axon Agent. For more information about the Axon Agent, see Getting Started with Tripwire Axon Agent on page 81.

- To install Axon Agent interactively, use the process starting with Step 1. Configuring the Axon Bridge below.
- To install Axon Agent silently, see Silent Installation of Axon Agent on page 94

**Step 1. Configuring the Axon Bridge**

**Note** The Axon Bridge only needs to be configured on a Tripwire Enterprise Server once, before connecting to an Axon Agent for the first time. If the Axon Bridge has already been configured (that is, the Bridge is already connected to an Axon Agent) proceed to Step 2. (Optional) Configuring a DNS SRV Record on page 85.

To configure the Axon Bridge on a Tripwire Enterprise Server:

1. Ensure that a supported version of Tripwire Enterprise Console is installed.
   
   The Axon Bridge is only supported on TE Console 8.5.0 or later.

2. On the system where Tripwire Enterprise Console is installed, open the following file in a text editor:

   `<te_root>/server/data/config/bridge_sample.properties`

3. Save a copy of this file with the name `bridge.properties` in the same directory.

4. In the `bridge.properties` file, complete the following steps:

   a. Locate the following line:

   ```
   #tw.cap.bridge.port=5670
   ```

   The Axon Bridge will 'listen' for incoming log messages from Axon Agents using port 5670 by default. If port 5670 is not available on the system where the Axon Bridge is installed, or you want to use another port, remove the pound sign (#) from the beginning of the line and replace 5670 with the new port number.

   b. Locate the following line:

   ```
   #tw.cap.bridge.registrationPreSharedKey=
   ```

   Remove the pound sign (#) from the beginning of the line and enter a **registration pre-shared key** of your choice. This pre-shared key is used by Axon Agent to register with the Tripwire Enterprise Server. The pre-shared key may include the space character and any alphanumeric characters, as well as the following special characters:

   "%$'\(*+,-./:;<=>?_"
c. By default, the Axon Bridge uses TLSv1.2 with cipher suites TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384. To change these settings, see Configuring TLS Versions for Axon Agent on page 103.

d. Save the file.

5. At a command prompt, enter the following command to restart the Bridge service:

```
<te_root>/server/bin/twserver restart
```

**Note** This command will restart the TE Console.

**Tip** If you encounter a problem with the Axon Bridge after configuration, review the Axon Bridge log file to assess the issue:

```
<te_root>/server/data/log/bridge.log
```

For additional assistance, contact Tripwire Support.
Step 2. (Optional) Configuring a DNS SRV Record

In a Domain Name System (DNS), an SRV record (or service record) defines the hostnames and port numbers of servers running various services. If you configure an SRV record for the system where the Axon Bridge is installed, Axon Agents can query the DNS server to determine the hostname and port number that the Bridge is using.

- **If a DNS SRV record already exists** for the Axon Bridge system, or **you do not want to use DNS SRV records** to configure Axon Agent, skip to *Step 3. Installing Axon Agent Software* on the next page.

- **To create a new DNS SRV record or edit an existing one**, follow the steps below.

To create or edit an SRV record on your DNS server:

1. On the DNS server, open the SRV record for a domain where Axon Agent will be installed. The name of the SRV record will appear in this format:

    
    _tw-agw._tcp.<domain_name>

    where `<domain_name>` is the name of the domain.

2. To specify the Tripwire Enterprise Server to which the Axon Agent will send data, enter the server's IP address or host name in the **Server Hostname** field.

3. In the **Port** field, enter the number of the port on the Tripwire Enterprise Server to be used for communication with Axon Agents. To use the default port, enter **5670**.


Step 3. Installing Axon Agent Software

In this step, you will install Axon Agent software on a host system. You must install Axon Agent software on each system that you want to monitor.

To install Axon Agent software, complete the appropriate steps for the Agent host system:

- *Installing Axon Agent on a Linux System (on the next page)*
- *Installing Axon Agent on a Windows System (on page 89)*

Caution: After installation, the Axon Agent will look for and use any _tw-agw_.tcp.<domain_name> DNS SRV record that exists for its DNS domain. This can be an issue if an existing DNS SRV record points to a different server, for example if Tripwire Enterprise and Tripwire Log Center are both installed in the same domain.

To resolve this issue, before installing Axon Agent software follow the steps in *Silent Installation of Axon Agent on page 94* to set the bridge.host setting in the Axon Agent's configuration file to point to the TE Console system.

Notes: TE Agent and Axon Agent cannot be installed on the same system. You must manually uninstall TE Agent from a system before installing Axon Agent. For more information, see *Uninstalling Tripwire Enterprise Agent on page 79*.

The TE Console software can only be upgraded if TE Agent is installed on the TE Console system. For this reason, Tripwire strongly recommends that you **not** install Axon Agent on the system where TE Console is installed.
Installing Axon Agent on a Linux System

This procedure will install Axon Agent and, optionally, the Event Generator software on a Linux system. An Event Generator is an auditing utility that supports audit event collection and real-time monitoring of this system by TE Console. For more information, see How Does an Event Generator Collect Audit Events? and How Does Real-Time Monitoring Work? in the Tripwire Enterprise User Guide.

To install Axon Agent software on a Linux system:

1. Confirm that Axon Agent is supported on the target system:

   http://www.tripwire.com/register/tripwire-axon-platform-support

2. Log in to the host system with a local administrator account.

   Note On Debian or Ubuntu systems, you can also use sudo to elevate privileges for the installing user.

3. Use one of the following command to install the software:

   RHEL or CentOS: rpm –ivh <installer_file>
   Debian or Ubuntu: dpkg –i <installer_file>

   where <installer_file> is the appropriate installer file (Table 19 below).

   **Table 19. Axon Agent installer files**

<table>
<thead>
<tr>
<th>File name</th>
<th>Target OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>axon-agent-installer-linux-x86.rpm</td>
<td>32-bit RHEL or CentOS systems</td>
</tr>
<tr>
<td>axon-agent-installer-linux-x64.rpm</td>
<td>64-bit RHEL or CentOS systems</td>
</tr>
<tr>
<td>axon-agent-installer-linux-x86.deb</td>
<td>32-bit Debian or Ubuntu systems</td>
</tr>
<tr>
<td>axon-agent-installer-linux-x64.deb</td>
<td>64-bit Debian or Ubuntu systems</td>
</tr>
</tbody>
</table>

4. (Optional) To install an Event Generator on this system, use one of the following commands to install the Event Generator driver and service:

   RHEL or CentOS: rpm –ivh <EG_driver_file> tw-eg-service*.rpm
   Debian or Ubuntu: dpkg -i <EG_driver_file> tw-eg-service*.deb

   where <EG_driver_file> is the appropriate driver file (Table 20 or Table 21 on the next page).

   Note On Ubuntu systems, only the DKMS Event Generator driver is supported, so tw-eg-driver-dkms*_all.deb should be installed.
Table 20. Axon Agent Event Generator driver files for RHEL and SUSE

<table>
<thead>
<tr>
<th>File name</th>
<th>Target OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>tw-eg-driver-rhel-*-i386.rpm</td>
<td>32-bit RHEL systems</td>
</tr>
<tr>
<td>tw-eg-driver-rhel-*-x86_64.rpm</td>
<td>64-bit RHEL systems</td>
</tr>
<tr>
<td>tw-eg-driver-suse-*-x86_64.rpm</td>
<td>64-bit SUSE systems</td>
</tr>
<tr>
<td>tw-eg-driver-dkms-*-noarch.rpm</td>
<td>32- and 64-bit RHEL systems with DKMS</td>
</tr>
</tbody>
</table>

1 This Event Generator driver can be installed with a DKMS package that will automatically rebuild the kernel driver every time the Linux kernel is upgraded. This makes the Event Generator more durable across Linux kernel updates.

In order to install the Event Generator driver DKMS package, you must first install DKMS. On RHEL and CentOS, this is provided through the EPEL repository, which you may need to enable. See https://fedoraproject.org/wiki/EPEL for more details. Once the EPEL repo configuration is imported and enabled, you can then use yum to install the DKMS package, which will automatically install additional dependencies such as gcc, kernel-devel, libgcc, and libgomp.

Caution: The kernel, kernel-header, and kernel-devel package versions must all be the same prior to installing the Event Generator DKMS driver, or the kernel module may not load.

Table 21. Axon Agent Event Generator driver files for Debian and Ubuntu

<table>
<thead>
<tr>
<th>File name</th>
<th>Target OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>tw-eg-driver-debian-*-x86.deb</td>
<td>32-bit Debian systems</td>
</tr>
<tr>
<td>tw-eg-driver-debian-*-x64.deb</td>
<td>64-bit Debian systems</td>
</tr>
<tr>
<td>tw-eg-driver-dkms-*-all.deb</td>
<td>32- and 64-bit Debian and Ubuntu systems with DKMS</td>
</tr>
</tbody>
</table>

1 This Event Generator driver can be installed with a DKMS package that will automatically rebuild the kernel driver every time the Linux kernel is upgraded. This makes the Event Generator more durable across Linux kernel updates. On Ubuntu systems, only the DKMS Event Generator driver is supported.

In order to install the Event Generator driver DKMS package, you must first install DKMS. You can use apt-get to install the DKMS package, which will automatically install additional dependencies such as gcc, dpkg-dev, coreutils, and make.

Caution: The linux-image and linux-header package versions must be the same prior to installing the Event Generator DKMS driver, or the kernel module may not load.
Installing Axon Agent on a Windows System

This procedure will install Axon Agent and the Event Generator software on a Windows system. An Event Generator is an auditing utility that supports audit event collection and real-time monitoring of this system by TE Console. For more information, see How Does an Event Generator Collect Audit Events? and How Does Real-Time Monitoring Work? in the Tripwire Enterprise User Guide.

To install Axon Agent software on a Windows system:

1. Confirm that Axon Agent is supported on the target system:
   
   http://www.tripwire.com/register/tripwire-axon-platform-support

2. Log in to the host system with a local administrator account.

3. To install the software in the default location (C:\Program Files\Tripwire\Agent), double-click the appropriate installer file (see Table 22 below) in the directory in which you unzipped the Axon Agent installation package.

To install the software in a different directory, open a command prompt and enter the following command:

   <installer_file> INSTALLDIR=<target_binary_installation_dir>

where

<installer_file> is the name of the appropriate installer file (see Table 22 below), and
<target_binary_file_directory> is the full path to the target installation directory

<table>
<thead>
<tr>
<th>File name</th>
<th>Target OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Axon_Agent_x86.msi</td>
<td>32-bit Windows systems</td>
</tr>
<tr>
<td>Axon_Agent_x64.msi</td>
<td>64-bit Windows systems</td>
</tr>
</tbody>
</table>

Note The Windows installer does not have a confirmation dialog for a successful installation. To verify that the Axon Agent has been installed correctly, check the Services list (Control Panel > Administrative Tools > View local services) to verify that the Tripwire Axon Agent service is running.
**Step 4. Configuring Axon Agent**

To configure an Axon Agent to communicate with the Tripwire Enterprise Server, you edit the Agent's configuration file `twagent.conf`. You must edit the configuration file on each system where Axon Agent is installed.

**To configure Axon Agent:**

1. Open one of the following files in a text editor:

   **Linux:**
   `/etc/tripwire/twagent_sample.conf`

   **Windows:**
   `%PROGRAMDATA%\Tripwire\agent\config\twagent_sample.conf`

   **Tip** For Windows systems, be sure to use the `%PROGRAMDATA%` path above, not Program Files.

2. Save a copy of this file with the name `twagent.conf` in the same directory.

3. If you **did not** configure an SRV record in **Step 2. (Optional) Configuring a DNS SRV Record on page 85**, you must manually enter the host name or IP address of the Tripwire Enterprise Server as the `bridge.host` option in the Axon Agent configuration file.

   `bridge.host=<product_server_hostname_or_IP>`

   If you **did** configure an SRV record, the Axon Agent will query the DNS Server when you restart the Axon Agent service (below). This query will attempt to identify an SRV record and use the hostname or IP address and port from the record to connect to the Axon Bridge. If the query is successful, the Agent's running configuration will use these values as the `bridge.host` and `bridge.port` options (see Table 23 on page 92).

4. As needed, edit the values of the other options in the Axon Agent configuration file (see Table 23 on page 92).

5. (Optional) To configure the Axon Agent to communicate through a SOCKS5 proxy, edit the values for the SOCKS5 settings. For more information, see Table 24 on page 93.

6. (Optional) By default, Axon Agent uses TLSv1.2 with cipher suites DHE-RSA-AES256-SHA:RSA-AES256-SHA:AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384. To change these settings, see **Configuring TLS Versions for Axon Agent on page 103**.

7. Create a text file named `registration_pre_shared_key.txt` and save the file in the following directory:

   **Linux:** `/etc/tripwire`
   **Windows:** `%PROGRAMDATA%\Tripwire\agent\config\`

8. In the text file, enter the same registration pre-shared key (value only) that you specified in the `bridge.properties` file in **Step 1. Configuring the Axon Bridge on page 83**.
9. (Optional) If you create a tag file for this Axon Agent, the tags in the file will automatically be assigned to this node when it is added to a TE Console. See Using Tag Files to Assign Tags to New Axon Agents on page 96 for more information.

Follow these steps to create a tag file:

   a. Create a text file named metadata.yml with the tags that you want to assign. For the file format, see Tag File Format for Axon Agents on page 97.

   b. Save the tag file to one of the following directories on the Axon Agent system:

      Linux: /etc/tripwire
      Windows: %PROGRAMDATA%\Tripwire\agent\config\%

10. (Optional) By default, an Event Generator installed with this Axon Agent communicates with the Agent using port 1169. To change the port used on this Agent, do the following:

   a. On the Axon Agent system, create a text file with the following line:
      \texttt{port=<new\_EG\_port>}

   b. Save the file to one of the following locations:

      Linux: /opt/tripwire/event-generator/service/tesvc.conf
      Windows: C:\Program Files\Tripwire\Agent\Event Generator Service\tesvc.conf
      (or an equivalent location if you installed Axon Agent to a different directory).

   c. Create another text file with the following line:
      \texttt{tesvc.port.control=<new\_EG\_port>}

      using the same port specified in the tesvc.conf file.

   d. Save the file to one of the following locations:

      Linux: /etc/tripwire/twfim.conf
      Windows: %PROGRAMDATA%\Tripwire\agent\config\twfim.conf

   e. Restart the Event Generator service:

      Linux: service tw-eg-service restart
      Windows: net stop TripwireEventGeneratorService & net start TripwireEventGeneratorService

11. At a command prompt, enter one of the following sets of commands to restart the Tripwire Axon Agent Service:

   **Linux (RHEL or CentOS):**
   
   /sbin/service tripwire-axon-agent stop
   /sbin/service tripwire-axon-agent start

   **Linux (Debian or Ubuntu):**
   
   /usr/sbin/service tripwire-axon-agent stop
   /usr/sbin/service tripwire-axon-agent start

   **Windows:**
   
   net stop TripwireAxonAgent
   net start TripwireAxonAgent
12. After completing these steps, you should see the Axon Agent in the TE Console Node Manager. For more information on using Axon Agent with Tripwire Enterprise, see the Tripwire Enterprise User Guide.

**Tip** If you encounter a problem with the Axon Agent after configuration, review the Axon Agent log file to assess the issue:

**Linux:**
/var/log/tripwire/twagent.log

**Windows:**
%PROGRAMDATA%\Tripwire\agent\log\twagent.log

For information on interpreting error messages, see *Axon Agent Error Messages* on page 110. For additional assistance, contact Tripwire Support.

### Table 23. Options in the Axon Agent configuration file

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge.host</td>
<td>The host name or IP address of the TE Server to which this Axon Agent will connect. For more information, see <em>Step 1. Configuring the Axon Bridge on page 83.</em></td>
</tr>
<tr>
<td>bridge.port</td>
<td>The port on the TE Server used for communication between the Axon Bridge and the Axon Agent. <strong>Default value:</strong> 5670</td>
</tr>
<tr>
<td>dns.service.domain</td>
<td>Specifies a DNS domain other than the Axon Agent host system's domain for SRV record lookup.</td>
</tr>
<tr>
<td>dns.service.name</td>
<td>Specifies a DNS service name. <strong>Default value:</strong> _tw-agw</td>
</tr>
<tr>
<td>registration.file.name</td>
<td>The name of the file containing the registration pre-shared key (defined in <em>Step 1. Configuring the Axon Bridge on page 83</em>) used by the Axon Agent to register with the Axon Bridge. <strong>Default value:</strong> registration_pre_shared_key.txt <strong>Note:</strong> The Axon Agent searches for the specified file name in one of the following directories: <strong>Linux:</strong> /etc/tripwire <strong>Windows:</strong> %PROGRAMDATA%\Tripwire\agent\config</td>
</tr>
<tr>
<td>spool.size.max</td>
<td>The maximum size of the spool with which the Axon Agent collects data from the Agent host system. <strong>Default value:</strong> 1GB</td>
</tr>
</tbody>
</table>
Table 24. SOCKS5 proxy options in the Axon Agent configuration file

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>socks5.host</td>
<td>The host name or IP address of the SOCKS5 proxy through which the Axon Agent communicates with the Axon Bridge.</td>
</tr>
<tr>
<td></td>
<td><strong>Default value:</strong> 1080</td>
</tr>
<tr>
<td>socks5.port</td>
<td>The port on the SOCKS5 proxy through which the Axon Agent communicates with the Axon Bridge.</td>
</tr>
<tr>
<td></td>
<td><strong>Default value:</strong> 1080</td>
</tr>
<tr>
<td>socks5.user.name</td>
<td>The username with which the Axon Agent will authenticate with the SOCKS5 proxy. If the SOCKS5 proxy is using username/password authentication, enter the username here and enter the password using the socks5.user.password setting. If the SOCKS5 proxy is using the &quot;no authentication&quot; method, leave this field and the socks5.user.password setting blank.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The password that the Axon Agent will use to authenticate with the SOCKS5 proxy if the proxy is using username/password authentication.</td>
</tr>
</tbody>
</table>

Table 25. TLS version and supported protocols in the Axon Agent configuration file

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tls.version</td>
<td>The TLS version used to connect with the Axon Bridge. Valid options are TLSv1, TLSv1.1, and TLSv1.2. Only one TLS version can be specified here. For information on changing the TLS version and cipher suites, see Configuring TLS Versions for Axon Agent on page 103. <strong>Default value:</strong> TLSv1.2</td>
</tr>
<tr>
<td>tls.cipher.suites</td>
<td>A colon-delimited list of cipher suites used by the Axon Agent when it connects to the Axon Bridge. Only OpenSSL FIPS-compatible cipher suites which utilize RSA keys are supported. <strong>Default value:</strong> DHE-RSA-AES256-SHA:RSA-AES256-SHA:AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384</td>
</tr>
</tbody>
</table>
Silent Installation of Axon Agent

With a silent installation of Axon Agent, you can easily automate the installation process for multiple systems. With the process below, you create a set of common files and then deploy them to each system where you want to install Axon Agent. After deploying these files, when Axon Agent is installed, it will connect with the Axon Bridge automatically.

Tip  You must install Axon Agent interactively at least once using the process in Installing Axon Agent on page 83 in order to get the twagent_sample.conf file that is used in the silent installation procedure below.

To silently install Axon Agent on a Linux or Windows system:

1. If you have not already done so, complete the following steps:
   - *Step 1. Configuring the Axon Bridge* (on page 83)
   - *Step 2. (Optional) Configuring a DNS SRV Record* (on page 85)

2. Create a common Axon Agent configuration file for all Axon Agents:
   a. On the system where you installed Axon Agent interactively, open one of the following files:
      - **Linux**: /etc/tripwire/twagent_sample.conf
      - **Windows**: %PROGRAMDATA%\Tripwire\agent\config\twagent_sample.conf
   b. If you didn't configure DNS SRV records, edit the bridge.host and bridge.port settings in the twagent_sample.conf file to specify the hostname and port of the Axon Bridge.
   c. (Optional) Edit other settings if necessary. You can find descriptions of these settings in the file.
   d. Save the file locally as twagent.conf.

3. Create a common registration pre-shared key file for all Axon Agents:
   a. Create a text file with the same registration pre-shared key (value only) that you specified in the bridge.properties file in *Step 1. Configuring the Axon Bridge on page 83.*
   b. Save the file locally as registration_pre_shared_key.txt.

4. (Optional) To assign Tripwire Enterprise tags to the Axon Agent systems, create a tag file:
   a. Create a text file with the tags that you want to assign. For the file format, see Tag File Format for Axon Agents on page 97.
   b. Save the file locally as metadata.yml.

5. On each Axon Agent target system, create one of the following directories:
   - **Linux**: /etc/tripwire
   - **Windows**: %PROGRAMDATA%\Tripwire\agent\config
6. Deploy the `metadata.yaml`, `twagent.conf`, and `registration_pre_shared_key.txt` files created above to the new directory on each Axon Agent target system.

7. Install Axon Agent on each target system as described in *Step 3. Installing Axon Agent Software* on page 86.

After installation, each Axon Agent system should connect with the Axon Bridge automatically.

**Tip**  
If you encounter a problem with any Axon Agent after configuration, review the Axon Agent log file to assess the issue:

**Linux:**  
```
/var/log/tripwire/twagent.log
```

**Windows:**  
```
%PROGRAMDATA%\Tripwire\agent\log\twagent.log
```

For information on interpreting error messages, see *Axon Agent Error Messages* on page 110. For additional assistance, contact Tripwire Support.
Using Tag Files to Assign Tags to New Axon Agents

Tag files can be deployed with new Axon Agent installations to simplify onboarding of new systems. A tag file is a text file on an Agent system that specifies tags to be assigned to the asset the first time it is added to a TE Console.

Tag files can be useful when automatic tagging profiles alone are not sufficient to tag assets, for example in cases when different assets share the same IP address or hostname.

<table>
<thead>
<tr>
<th>Notes</th>
<th>For more information on tags, tagging profiles, and how they can be used in TE, see Getting Started with Tags in the Tripwire Enterprise User Guide.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>While tag files work the same way on TE Agents and Axon Agents, the implementation and file format are slightly different. For information on using tag files with TE Agents, see Using Tag Files to Assign Tags to New TE Agents on page 72.</td>
</tr>
</tbody>
</table>

Consider the following points when using tag files:

- Specific instructions for deploying tag files on Axon Agent are in Step 4. Configuring Axon Agent on page 90.

- Tag files must be named metadata.yml, and must be in one of the following directories on the Axon Agent system:
  
  **Linux:** /etc/tripwire  
  **Windows:** %PROGRAMDATA%\Tripwire\agent\config\%

- The format for a tag file is specified in Tag File Format for Axon Agents (on the next page).

- A tag file must be present before the Agent has started for the first time, and the tags in the file are only assigned the first time the asset is added to a TE Console. Subsequent restarts will not add tags or modify the tags already assigned.

- Tags in a tag file are added in addition to the system tags (Operating System, Status, etc.) that are automatically assigned when an asset is added to TE Console.

- Tags and tag sets used in the tag file must already exist within a TE Console when the asset is added. If new tags or tag sets are included in a tag file, no tags in the file will be assigned, and the Console will generate an error.

- Only user-created tags and tag sets can be added using a tag file. If system tag sets or operational tag sets are included in a tag file, they will be ignored.

- If an asset's tag file contains errors when it is added to TE Console, the asset is tagged with a Health:Uncategorized Error tag. In addition, an error message with the category Asset View Change will be added to the Log Manager and `teserver.log` file.

- Tag files with double-byte characters must be encoded with UTF8 or UTF16 (with a byte order mark).
Tag File Format for Axon Agents

Tag files for Axon Agents are written in YAML format ([www.yaml.org](http://www.yaml.org)) and have the following structure:

```
{
    tagSets :
    {
        tagSet1 : [tag1, tag2, etc],
        tagSet2 : [tag1, tag2, etc],
        # etc
    }
}
```

For example:

```
{
    tagSets :
    {
        Location : [Portland],
        Importance : [Critical],
        Policy : [CIS, PCI]
    }
}
```

Comments can be included in the tag file if they are preceded by a # character. For example:

```
# Here are the tags for Axon Agents
```

For more information about the acceptable characters and formatting in a tag file for Axon Agents, see the YAML format page at [www.yaml.org](http://www.yaml.org).
Upgrading Axon Agent

Axon Agent software is upgraded by running a RPM, DEB, or MSI installation file on a system where Axon Agent is already installed.

**Notes**

Axon Agent software cannot be upgraded from the TE Console. Use the process below to upgrade the software on each Agent's host system.

For TE Agent upgrade instructions, see *Upgrading Tripwire Enterprise Agent* on page 76.

### To upgrade the Axon Agent to the latest version, complete the following steps:

1. Determine the version of Axon Agent that is currently installed by checking one of the following files on the Axon Agent system:
   
   **Linux:** `/opt/tripwire/agent/version`
   
   **Windows:** `%PROGRAMFILES%\tripwire\agent\version`

2. Check the **Downloads** page of the Tripwire Customer Center to see the latest version of Axon Agent that is available:

   ```
   https://tripwireinc.force.com/customers
   ```

   If the latest version is already installed on the Agent host system, no upgrade is necessary.

3. Download the installer file, and save it in a directory accessible from the Axon Agent host system.

4. Launch the Axon Agent installer you downloaded on the Agent host system.

   **Linux:**
   
   a. Log in with root privileges (or use `sudo` on Debian or Ubuntu systems to obtain root privileges).
   
   b. Run one of the following sets of commands:

   ```
   RHEL or CentOS:
   rpm -U <installer_rpm_file>
   /sbin/service tripwire-axon-agent start
   ```

   ```
   Debian or Ubuntu:
   dpkg -i <installer_deb_file>
   /usr/sbin/service tripwire-axon-agent start
   ```

   **Windows:**

   a. Log in with a local administrator account.

   b. Open the directory containing the installer (.msi) file and double-click the file.
5. (Optional) An **Event Generator** is an auditing utility that supports audit event collection and real-time monitoring of an Axon Agent system by TE Console. On Windows systems, it is installed and enabled automatically with the Axon Agent software. On Linux systems, you must install it manually if you want to collect audit events or monitor the Axon Agent in real time.

To upgrade an Event Generator on a Linux system, use one of the following commands:

**RHEL or CentOS:** `rpm -U <EG_driver_file> tw-eg-service*.rpm`

**Debian or Ubuntu:** `dpkg -i <EG_driver_file> tw-eg-service*.deb`

where `<EG_driver_file>` is the appropriate driver file (Table 26 below or Table 27 on the next page).

| Note | On Ubuntu systems, only the DKMS Event Generator driver is supported, so `tw-eg-driver-dkms_*_all.deb` should be installed. |

### Table 26. Axon Agent Event Generator driver files for RHEL and SUSE

<table>
<thead>
<tr>
<th>File name</th>
<th>Target OS</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tw-eg-driver-rhel-*.i386.rpm</code></td>
<td>32-bit RHEL systems</td>
</tr>
<tr>
<td><code>tw-eg-driver-rhel-*.x86_64.rpm</code></td>
<td>64-bit RHEL systems</td>
</tr>
<tr>
<td><code>tw-eg-driver-suse-*.x86_64.rpm</code></td>
<td>64-bit SUSE systems</td>
</tr>
<tr>
<td><code>tw-eg-driver-dkms-*.noarch.rpm</code></td>
<td>32- and 64-bit RHEL systems with DKMS ¹</td>
</tr>
</tbody>
</table>

¹ This Event Generator driver can be installed with a DKMS package that will automatically rebuild the kernel driver every time the Linux kernel is upgraded. This makes the Event Generator more durable across Linux kernel updates.

In order to install the Event Generator driver DKMS package, you must first install DKMS. On RHEL and CentOS, this is provided through the EPEL repository, which you may need to enable. See [https://fedoraproject.org/wiki/EPEL](https://fedoraproject.org/wiki/EPEL) for more details. Once the EPEL repo configuration is imported and enabled, you can then use `yum` to install the DKMS package, which will automatically install additional dependencies such as `gcc`, `kernel-devel`, `libgcc`, and `libgomp`.

**Caution:** The kernel, kernel-header, and kernel-devel package versions must all be the same prior to installing the Event Generator DKMS driver, or the kernel module may not load.
Table 27. Axon Agent Event Generator driver files for Debian and Ubuntu

<table>
<thead>
<tr>
<th>File name</th>
<th>Target OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>tw-eg-driver-debian-*-x86.deb</td>
<td>32-bit Debian systems</td>
</tr>
<tr>
<td>tw-eg-driver-debian-*-x64.deb</td>
<td>64-bit Debian systems</td>
</tr>
<tr>
<td>tw-eg-driver-dkms-*-all.deb</td>
<td>32- and 64-bit Debian and Ubuntu systems with</td>
</tr>
<tr>
<td></td>
<td>DKMS¹</td>
</tr>
</tbody>
</table>

¹ This Event Generator driver can be installed with a DKMS package that will automatically rebuild the kernel driver every time the Linux kernel is upgraded. This makes the Event Generator more durable across Linux kernel updates. On Ubuntu systems, only the DKMS Event Generator driver is supported.

In order to install the Event Generator driver DKMS package, you must first install DKMS. You can use apt-get to install the DKMS package, which will automatically install additional dependencies such as gcc, dpkg-dev, coreutils, and make.

**Caution:** The `linux-image` and `linux-header` package versions must be the same prior to installing the Event Generator DKMS driver, or the kernel module may not load.
Uninstalling Axon Agent

To uninstall Axon Agent from a Windows system:

1. Log in to the system with Administrator privileges.
2. Open the Windows Control Panel.
3. In the Control Panel, open Programs and Features.
4. Select Axon Agent and click Uninstall.
5. If you do not plan to re-install Axon Agent, delete the following directories:

   \%ProgramFiles\%Tripwire\Agent
   \%PROGRAMDATA\%Tripwire\agent

To uninstall Axon Agent from a Linux system:

1. Log in to the system as root (or use sudo on Debian or Ubuntu systems to obtain root privileges).
2. At a command prompt, enter one of the following commands:

   **RHEL or CentOS:** rpm -e axon-agent
   **Debian or Ubuntu:** dpkg -r axon-agent

3. If an Event Generator is installed, enter one of the following commands to remove the Event Generator driver and service:

   **RHEL or CentOS:** rpm -e <event_generator_package> tw-eg-service
   **Debian or Ubuntu:** dpkg -r <event_generator_package> tw-eg-service

   where <event_generator_package> is one of the packages in **Table 28**.

**Table 28. Axon Agent Event Generator packages**

<table>
<thead>
<tr>
<th>Package name</th>
<th>Target OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>tw-eg-driver-rhel</td>
<td>RHEL systems</td>
</tr>
<tr>
<td>tw-eg-driver-suse</td>
<td>SUSE systems</td>
</tr>
<tr>
<td>tw-eg-driver-debian</td>
<td>Debian systems</td>
</tr>
<tr>
<td>tw-eg-driver-dkms</td>
<td>Systems with the DKMS Event Generator driver</td>
</tr>
</tbody>
</table>

4. If you do not plan to re-install Axon Agent, delete the following directories:

   /etc/tripwire
   /opt/tripwire/agent
   /var/cache/tripwire
   /var/lock/tripwire
   /var/log/tripwire
   /var/spool/tripwire
Other Axon Agent Procedures

Determining an Axon Agent's Version

The simplest way to determine the version of Axon Agent that is installed is to check one of the following files on the Axon Agent system:

- **Linux:** /opt/tripwire/agent/version
- **Windows:** %PROGRAMFILES%\tripwire\agent\version

To determine the version of the Event Generator that is installed, use one of these procedures:

**To determine the version of Axon Agent that is installed on a Linux system:**

1. Log in to the system with administrator privileges (or use **sudo** on Debian or Ubuntu systems to obtain root privileges).
2. Run one of the following commands and check the Version field:
   - **RHEL or CentOS:** # rpm -qi axon-agent
   - **Debian or Ubuntu:** # dpkg -s axon-agent
3. To determine the version of the Event Generator that is installed, run:
   - **RHEL or CentOS:** # rpm -qi <event_generator_package> tw-eg-service
   - **Debian or Ubuntu:** # dpkg -s <event_generator_package> tw-eg-service

where `<event_generator_package>` is one of the packages in **Table 29.**

<table>
<thead>
<tr>
<th>Package name</th>
<th>Target OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>tw-eg-driver-rhel</td>
<td>Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>tw-eg-driver-suse</td>
<td>SUSE Linux</td>
</tr>
<tr>
<td>tw-eg-driver-debian</td>
<td>Debian systems</td>
</tr>
<tr>
<td>tw-eg-driver-dkms</td>
<td>Systems with the DKMS Event Generator driver</td>
</tr>
</tbody>
</table>

**To determine the version of Axon Agent that is installed on a Windows system:**

1. Log in to the system with Administrator privileges, and open the Windows Control Panel.
2. In the Control Panel, open **Add / Remove Programs** or **Programs and Features**.
3. Select **Axon Agent**, and check the **Version** field.

**Note** The Event Generator on Windows systems does not have a separate version number.
Configuring TLS Versions for Axon Agent

This section describes the process to change the TLS version and cipher suites used by Axon Agents and the Axon Bridge. For more information on supported TLS versions and cipher suites, see Supported TLS Versions and Cipher Suites on page 105.

To change the TLS version and cipher suites used:

1. On the Tripwire Enterprise Server, open the following file in a text editor:
   
   `<te_root>/server/data/config/bridge.properties`

2. To configure the **TLS versions** that the Axon Bridge will use to accept connections from an Axon Agent, edit the `tw.cap.bridge.tlsVersion` value. To configure the Bridge to accept connections using only a single TLS version, specify it like this:

   ```
   tw.cap.bridge.tlsVersion=TLSv1.2
   ```

   To configure the Axon Bridge to accept connections using more than one version of TLS, specify all of the accepted versions as a comma-separated list. For example:

   ```
   tw.cap.bridge.tlsVersion=TLSv1.2,TLSv1.1,TLSv1
   ```

3. To configure the **TLS cipher suites** that the Axon Bridge will use, edit the `tw.cap.bridge.tlsCipherSuites` value. For a list of values, see Table 30 on page 105.

   To configure multiple cipher suites, specify them as a comma-separated list. For example:

   ```
   tw.cap.bridge.tlsCipherSuites=TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
   ```

4. Save the `bridge.properties` file.

5. At a command prompt, enter the following command to restart the Tripwire Bridge Service:

   ```
   <te_root>/server/bin/twserver restart
   ```

   **Note** This command will restart the TE Console.

6. On each Axon Agent where you want to change the TLS version and/or cipher suites, do the following:

   a. Open one of the following files in a text editor:

      Linux: `/etc/tripwire/twagent.conf`
      Windows: `%PROGRAMDATA%\Tripwire\agent\config\twagent.conf`

   b. To configure the single **TLS version** that this Axon Agent will use to connect with the Axon Bridge, edit the `tls.version` value. For example:

      ```
      tls.version=TLSv1.2
      ```
c. To configure the **TLS cipher suites** that this Axon Agent will use, edit the `tls.cipher.suites` value. For a list of values, see Table 30 on the next page.

   To configure multiple cipher suites, specify them as a colon-separated list. For example:

   ```
   ```

   **Note**  
   If the Axon Agent attempts to connect with an Axon Bridge that does not support any of the specified TLS ciphers, the TLS handshake will fail and the connection will be closed.

   **Note**  
   If the Axon Agent attempts to connect with an Axon Bridge that does not support the specified TLS protocol, the TLS handshake will fail and the connection will be closed.

d. At a command prompt, enter one of the following sets of commands to restart the Tripwire Axon Agent Service:

**Linux (RHEL and CentOS):**
```
/sbin/service tripwire-axon-agent stop
/sbin/service tripwire-axon-agent start
```

**Linux (Debian and Ubuntu):**
```
/usr/sbin/service tripwire-axon-agent stop
/usr/sbin/service tripwire-axon-agent start
```

**Windows:**
```
net stop TripwireAxonAgent
net start TripwireAxonAgent
```
Supported TLS Versions and Cipher Suites

Axon Agents and the Axon Bridge support TLSv1, TLSv1.1, and TLSv1.2.

Both Axon Agents and the Axon Bridge use TLSv1.2 by default. Table 30 lists the default cipher suites configured by the Axon Bridge and by Axon Agents. Note that the same cipher suites are supported in both places, but the names are different because the Axon Bridge uses Java cipher suite names, while Axon Agents use OpenSSL names.

The Axon Bridge and Axon Agents can use any TLS cipher suite that is implemented by both Java and OpenSSL, and that is allowed by Federal Information Processing Standards (FIPS) 140-2.

Table 30. List of default cipher suites

<table>
<thead>
<tr>
<th>Cipher Suite Name on the Axon Bridge</th>
<th>Corresponding Name on an Axon Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</td>
<td>DHE-RSA-AES256-SHA</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA</td>
<td>RSA-AES256-SHA</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_GCM_SHA384</td>
<td>AES256-GCM-SHA384</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>DHE-RSA-AES256-GCM-SHA384</td>
</tr>
</tbody>
</table>
Changing the TE Console Used to Manage an Axon Agent

To change the TE Console used to manage an Axon Agent:

1. Complete the following steps on the new Tripwire Enterprise Server:
   a. If needed, upgrade to the latest version of Tripwire Enterprise Console.
   b. Configure the Bridge, as described in Step 1. Configuring the Axon Bridge on page 83.

2. Complete the following steps on the Axon Agent host system:
   a. Shut down the Tripwire Axon Agent service by entering one of the following commands:

   **Linux (RHEL and CentOS):** `/sbin/service tripwire-axon-agent stop`
   **Linux (Debian and Ubuntu):** `/usr/sbin/service tripwire-axon-agent stop`
   **Windows:** `net stop TripwireAxonAgent`

   b. Delete the following certificates.

   **Linux:** `/var/cache/tripwire/trust/keystore.p12`
   **Windows:** `%PROGRAMDATA%\Tripwire\agent\data\trust\keystore.p12`

   c. Open the Axon Agent configuration file (`twagent.conf`) in the appropriate directory.

   **Linux:** `/etc/tripwire/`
   **Windows:** `%PROGRAMDATA%\Tripwire\agent\config\`

   d. In the configuration file, enter the IP address or host name of the new Tripwire Enterprise Server as the `bridge.host` option, and edit the other options, as needed (see Table 23 on page 92).

   e. Create a text file named `registration_pre_shared_key.txt` and save the file in the following directory:

   **Linux:** `/etc/tripwire/`
   **Windows:** `%PROGRAMDATA%\Tripwire\agent\config\`

   f. In the text file, enter the registration pre-shared key (value only) for the new Agent Bridge.

   g. Start the Tripwire Axon Agent service by entering one of the following commands at a command prompt.

   **Linux (RHEL and CentOS):** `/sbin/service tripwire-axon-agent start`
   **Linux (Debian and Ubuntu):** `/usr/sbin/service tripwire-axon-agent start`
   **Windows:** `net start TripwireAxonAgent`
Revoking an Axon Agent's Certificate

If the Axon Bridge is running in registration mode on the TE Server (the default setting; see Step 1. Configuring the Axon Bridge on page 83), the Bridge maintains a list of certificates granted to connecting Axon Agents. If an Axon Agent's certificate is revoked, the TE Server will deny SSL connection requests from the Agent.

To revoke an Axon Agent's certificate:

1. To identify the Axon Agent's Universally Unique Identifier (UUID), run one of the following commands on the Agent host system.

   **Linux**: `/opt/tripwire/agent/tools/twagent/twagentstat --dump.uuid.dat`

   **Windows**: `"%PROGRAMFILES%\Tripwire\Agent\tools\twagent\twagentstat" --dump.uuid.dat`

   **Tip** Alternatively, you can determine the Axon Agent's UUID by opening the Axon Bridge Log on the TE Server:

   `<te_root>/server/data/log/bridge.log`

   Search the log for the IP address used by the Agent to connect to the Bridge. The Agent's UUID should appear in a message similar to the following:


2. Run the following commands on the TE Server:

   a. To determine if the Axon Agent's certificate has already been revoked, run:

      ```
      cd <te_root>/server/sup/crl/bin
      agentCrlManager -d ../../../data/bridge list
      ```

   b. To revoke the Axon Agent's certificate, run:

      ```
      agentCrlManager -d ../../../data/bridge revoke --agent <UUID>
      ```

      where `<UUID>` is the Axon Agent's Universally Unique Identifier (UUID).

   c. To restart the Tripwire Bridge Service, run:

      ```
      <te_root>/server/bin/twserver restart
      ```

      **Note** This command will restart the TE Console.
Troubleshooting Axon Agent

This section lists troubleshooting procedures for Axon Agent, a list of Axon Agent error messages with resolutions, and instructions for creating a diagnostic support bundle for Tripwire Support.

Troubleshooting Procedures

If you encounter difficulties with an Axon Agent, complete the following steps:

1. To confirm that the collection binaries are running, run the appropriate command on the Axon Agent host system:
   
   **Linux:** `ps -ef`
   
   **Windows:** `tasklist`

2. To confirm that the Axon Agent has an open connection to the Axon Bridge on the TE Server (using port 5670, the default), run the appropriate command on the Axon Agent host system:
   
   **Linux:** `netstat -an | grep 5670`
   
   **Windows:** `netstat -an | findstr 5670`

3. Open the Axon Agent log file (`twagent.log`):
   
   **Linux:** `/var/log/tripwire/twagent.log`
   
   **Windows:** `%PROGRAMDATA%\Tripwire\agent\log\twagent.log`

### Table 31. List of Axon Agent executables

<table>
<thead>
<tr>
<th>Executable name</th>
<th>On Linux Agents?</th>
<th>On Windows Agents?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>twagent</td>
<td>Y</td>
<td>Y</td>
<td>Axon Agent service</td>
</tr>
<tr>
<td>twexec</td>
<td>Y</td>
<td>Y</td>
<td>Command collector</td>
</tr>
<tr>
<td>twfim</td>
<td>Y</td>
<td>Y</td>
<td>File and Registry collector</td>
</tr>
<tr>
<td>twforager</td>
<td>Y</td>
<td>Y</td>
<td>System information collector</td>
</tr>
<tr>
<td>twrsop</td>
<td></td>
<td>Y</td>
<td>Windows policy collector</td>
</tr>
<tr>
<td>twsupport</td>
<td>Y</td>
<td>Y</td>
<td>Support bundle collector</td>
</tr>
<tr>
<td>twtail</td>
<td>Y</td>
<td>Y</td>
<td>Advanced file collector</td>
</tr>
<tr>
<td>twwel</td>
<td></td>
<td>Y</td>
<td>Advanced Windows collector</td>
</tr>
</tbody>
</table>

**Note** Plugins will not be listed if they are not currently in use.
To interpret the messages in the Axon Agent log file, see *Axon Agent Error Messages on the next page*.

4. To confirm that the Axon Bridge is listening for Axon Agents (using port 5670, the default port), run the appropriate command on the TE Server:

**Linux:** `netstat -an | grep 5670`
**Windows:** `netstat -an | findstr 5670`

**Determining the Locale on Linux Axon Agents**

On Linux Axon Agents, the locale is determined by the settings in the default language configuration file:

- **CentOS:** `/etc/sysconfig/i18n`
- **RHEL:** `/etc/sysconfig/i18n`
- **SuSE:** `/etc/sysconfig/language`
- **Debian:** `/etc/default/locale`
- **Ubuntu:** `/etc/default/locale`
Axon Agent Error Messages

Table 32 lists error messages that you may encounter when configuring and using Axon Agent. You can find these error messages in the Axon Agent log files:

Linux:
/var/log/tripwire/twagent.log

Windows:
%PROGRAMDATA%\Tripwire\agent\log\twagent.log

Table 32. Axon Agent error messages

<table>
<thead>
<tr>
<th>Error message:</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARN twagent.bridge BridgeTLSConnector::connect_() - No bridge endpoints to connect to. Rescanning...</td>
</tr>
<tr>
<td>Cause:</td>
</tr>
<tr>
<td>The Axon Agent is unable to determine the Axon Bridge to connect to.</td>
</tr>
<tr>
<td>Resolution:</td>
</tr>
<tr>
<td>1) Check the bridge.host setting in the Axon Agent's twagent.conf file.</td>
</tr>
<tr>
<td>2) Check the Bridge system's DNS and DNS SRV record.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error messages (Windows):</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR twagent.bridge BridgeTLSConnector::handleConnectTimeOut() - Connect Timeout reached secs: [20], state=Connector::Failed</td>
</tr>
<tr>
<td>twagent.bridge BridgeTLSConnector::handleConnect() - Failed, error:[system:121</td>
</tr>
<tr>
<td>Cause:</td>
</tr>
<tr>
<td>The Axon Agent is unable to connect with the Axon Bridge.</td>
</tr>
<tr>
<td>Resolution:</td>
</tr>
<tr>
<td>Check your firewalls and network routing configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error messages (Linux):</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR twagent.bridge BridgeTLSConnector::handleAnonymousHandshake() - Failed Connecting to host.example.com:5670, Error: [system: 104</td>
</tr>
<tr>
<td>ERROR twagent.bridge BridgeTLSConnector::handleConnect() - Failed, error:[system:111</td>
</tr>
<tr>
<td>Cause:</td>
</tr>
<tr>
<td>The Axon Agent is unable to connect with the Axon Bridge.</td>
</tr>
<tr>
<td>Resolution:</td>
</tr>
<tr>
<td>Check your firewalls and network routing configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error message:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR twagent.bridge BridgeTLSConnector::handleAgentRegistrationResponse_() - Registration error, status value:[ERROR_INCORRECT_KEY], message: &quot;The registration pre-shared key is incorrect.&quot;, Disconnecting...</td>
</tr>
<tr>
<td>Cause:</td>
</tr>
<tr>
<td>The registration pre-shared key on the Axon Bridge does not match the key that Axon Agents are using to authenticate and request certificates.</td>
</tr>
<tr>
<td>Resolution:</td>
</tr>
<tr>
<td>Verify that the registration pre-shared key configured on the Axon Bridge matches the pre-shared key in the registration_pre_shared_key.txt file that the Axon Agent is attempting to authenticate with.</td>
</tr>
</tbody>
</table>
### Error messages:
- **WARN** twagent::sslInfoCallback() - TLSv1.2 write alert: fatal:unknown CA

- **ERROR** twagent::bridge::BridgeTLSConnector::handleHandshake() - Failed Connecting to host.example.com:5670, Error: [asio.ssl: 336134278 | certificate verify failed]

**Cause:**
The certificate being used by the Axon Bridge and an Axon Agent have different CA's. This can happen when Axon Agents are moved between different Bridges.

**Resolution:**
Follow the process in *Changing the TE Console Used to Manage an Axon Agent on page 130* to re-authenticate the Axon Agent with this Axon Bridge.

### Error message:
**ERROR** twagent::bridge::BridgeTLSConnector::handleHandshake() - Failed Connecting to host.example.com:5670, Error: [asio.ssl: 336151574 | sslv3 alert certificate unknown]

**Cause:**
The certificate for an Axon Agent has been revoked on the Axon Bridge.

**Resolution:**
Follow the process in *Changing the TE Console Used to Manage an Axon Agent on page 130* to re-authenticate the Axon Agent with this Axon Bridge.

### Error message:
**ERROR** twagent::bridge::BridgeTLSConnector::handleAnonymousHandshake() - Failed Connecting to host.example.com:5670, Error: [asio.ssl: 336130315 | wrong version number]

**Cause:**
The Axon Bridge and the Axon Agent do not have a TLS version in common.

**Resolution:**
Follow the process in *Configuring TLS Versions for Axon Agent on page 103* to configure a common TLS version on the Axon Bridge and Axon Agents.

### Error messages:
- **ERROR** twagent::bridge::BridgeTLSConnector::handleAnonymousHandshake() - Failed Connecting to host.example.com:5670, Error: [asio.ssl: 336151568 | sslv3 alert handshake failure]

- **ERROR** twagent::bridge::BridgeTLSConnector::handleAnonymousHandshake() - Failed Connecting to host.example.com:5670, Error: [asio.ssl: 336081077 | no ciphers available]

**Cause:**
The Axon Bridge and the Axon Agent do not have a TLS cipher suite in common.

**Resolution:**
Follow the process in *Configuring TLS Versions for Axon Agent on page 103* to configure one or more common TLS cipher suites on the Axon Bridge and Axon Agents.
Creating a Support Bundle

To create a support bundle for analysis by Tripwire Support, run the appropriate command on the Axon Agent host system.

**Linux:**

```
/opt/tripwire/agent/plugins/twsupport/twsupport --generate.bundle=<zip_file>
```

**Windows:**

```
"<Program_Files>\Tripwire\Agent\plugins\twsupport\twsupport"
--generate.bundle=<zip_file>
```

where `<zip_file>` is the support bundle zip file to be created.
Configuring Tripwire Enterprise Inside a Network Address Translation (NAT) Environment

Network Address Translation (NAT) is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. Positioned between the LAN and the Internet, a NAT server translates any internal IP addresses embedded in communications that pass between internal and external systems. By preventing the exposure of internal IP addresses to external sources, NAT enhances the security of an organization’s network.

**Note** A DNS server is not required for a Tripwire Enterprise (TE) implementation in a NAT environment. However, if your environment does use DNS, be sure that each TE system outside of the NAT resolves the system’s hostname to the NAT server’s IP address. In other words, the TE system inside the NAT must resolve the hostname to itself.

To configure a Tripwire Enterprise system (either a TE Server or TE Agent) positioned inside a NAT environment:

1. Configure the NAT server to forward inbound communications to the RMI and HTTP ports (9898 and 8080 by default) used by TE.

2. On the TE system:
   a. Open the hosts file. By default, this file is stored in the following directories.
      
      Windows: \WINDOWS\System32\drivers\etc\
      
      UNIX/Linux/OS X: /etc/
   b. Delete any external hostnames in the 127.0.0.1 loopback line.
   c. Add the following line:
      
      `<TE_system_IP_address> <TE_system_FQDN> <TE_system_hostname>`
      
      For example:
      
      10.0.0.1 internal.mycompany.com internal
      
      For variable definitions, see Table 33 below.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;TE_system_IP_address&gt;</code></td>
<td>The IP address of the TE system inside the NAT (either a TE Server or TE Agent).</td>
</tr>
<tr>
<td><code>&lt;TE_system_FQDN&gt;</code></td>
<td>The fully-qualified domain name of the TE system inside the NAT.</td>
</tr>
<tr>
<td><code>&lt;TE_system_hostname&gt;</code></td>
<td>The hostname of the TE system inside the NAT.</td>
</tr>
<tr>
<td><code>&lt;NAT_IP_address&gt;</code></td>
<td>The IP address of the NAT server.</td>
</tr>
</tbody>
</table>
3. On each Tripwire Enterprise system outside of the NAT:
   a. Open the hosts file.
   b. Delete any external hostnames in the 127.0.0.1 loopback line.
   c. Enter the following line:
      `<NAT_IP_address> <TE_system_FQDN> <TE_system_hostname>`
      For example:
      `100.3.2.1 internal.mycompany.com internal`

4. On a TE Agent system inside the NAT, configure the system’s configuration file:
   a. Open the `agent.properties` file. By default, this file is stored in:
      `<te_root>/agent/data/config/`
   b. Add the following property:
      `java.rmi.server.hostname=<TE_system_FQDN>`
      For example:
      `java.rmi.server.hostname=internal.mycompany.com`
   c. Save and close the `agent.properties` file.

5. Restart the TE service on the system inside the NAT. For instructions, see:
   - *Managing Tripwire Enterprise Console Services* (on page 133)
   - *Managing the Tripwire Enterprise Agent Service* (on page 134)
Configuring a Tripwire Enterprise Agent for Use on a Multi-NIC System

A Tripwire Enterprise Server can communicate with TE Agents via a network interface card (NIC) other than the primary/default interface.

To configure a Tripwire Enterprise Agent for use with multiple NICs:

1. On the system where the TE Agent is installed, log in as the root user (UNIX/Linux/OS X) or as Administrator (Windows).

2. Stop the TE Agent service (see Managing the Tripwire Enterprise Agent Service on page 134).

3. Open the agent.properties file and add the following lines:
   
   ```
   tw.rpc.interfaceAddr=<NIC_IP_address>
   java.rmi.server.hostname=<NIC_FQDN>
   ```

   where

   `<NIC_IP_address>` is the IP address that the Agent will listen on. If not specified, the Agent will listen on any local IP address

   and

   `<NIC_FQDN>` is the fully-qualified domain name of the NIC used by the TE Server for connections to the Agent.

4. Save and close the agent.properties file.

5. Restart the TE Agent service (see Managing the Tripwire Enterprise Agent Service on page 134).
Configuring a Tripwire Enterprise Proxy for Agent Communication

A Tripwire Enterprise (TE) proxy is a TE Agent system that enables your TE Server to communicate with other TE Agent systems on the other side of a firewall. If you create and configure a TE proxy, all communications between your TE Server and specified TE Agents will pass through the proxy, thereby bypassing the firewall.

Note: Axon Agents use a SOCK5 proxy instead of a TE proxy. To configure a proxy for Axon Agents, see Step 4. Configuring Axon Agent on page 90.

To configure a TE proxy, complete the following steps:

- Step 1. Configuring Your Tripwire Enterprise Server (below)
- Step 2. Installing and Configuring the Tripwire Enterprise Proxy (on the next page)
- Step 3. Configuring TE Agents for Communication with the Proxy (on page 119)
- Step 4. Configuring the Firewall (on page 120)

Step 1. Configuring Your Tripwire Enterprise Server

If any of the TE Agents that will use the TE proxy are unable to resolve the hostname of your TE Server, complete the steps below. Otherwise, proceed to Step 2. Installing and Configuring the Tripwire Enterprise Proxy on the next page.

To configure your Tripwire Enterprise Server for a TE proxy:

1. On the TE Server, open the TE Console configuration file:
   
   `<te_root>/server/data/config/server.properties`

2. If the proxy has multiple NICs, and the TE Agents and TE Server are on different subnets, set the following property to inform the TE Server of the IP addresses used by the TE Agents to communicate with the proxy:

   `tw.proxy.nicMap = <server1_proxy>:<agent1_proxy>,<agent2_proxy>, ...
   
   where:

   `<server1_proxy>` is the IP address used by the TE Server to communicate with the proxy,
   `<agent1_proxy>` is the IP address used by the first Agent to communicate with the proxy, and
   `<agent2_proxy>` is the IP address used by the second Agent to communicate with the proxy

   To configure multiple proxies, insert a bar (|) between the proxy addresses. For example:

   `tw.proxy.nicMap = <server1_proxy>:<agent1_proxy>,<agent2_proxy> | \
   <server2_proxy>:<agent3_proxy>,<agent4_proxy>`

   where \ is a line-continuation character.

3. Restart the TE Console service (see Managing Tripwire Enterprise Console Services on page 133).
Step 2. Installing and Configuring the Tripwire Enterprise Proxy

In this step, you will install and configure Tripwire Enterprise Agent software on your proxy system. The proxy system must be able to resolve the hostname of your TE Server.

To install and configure your TE proxy:

1. Install Tripwire Enterprise Agent software on the TE proxy system. For more information, see Chapter 2: Installing Tripwire Enterprise Agent (on page 39).

2. Open the Agent configuration file on the TE proxy system:

   <te_root>/agent/data/config/agent.properties

3. Add socksProxy to the space.bootstrapables property. For example:

   space.bootstrapables=station,socksProxy

4. Enter (or confirm) the value of each property listed in Table 34 below.

Table 34. Properties for the TE proxy system

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>java.rmi.server.hostname</td>
<td>The fully-qualified domain name of the NIC used by the TE Server for connections to the TE Agent.</td>
</tr>
<tr>
<td>tw.proxy.serverPort</td>
<td>The port on the TE proxy that will receive proxy requests from TE Agents and the TE Server (default = 1080).</td>
</tr>
<tr>
<td>tw.rpc.interfaceAddr</td>
<td>If your TE proxy is multi-NIC with multiple domain names, enter the domain name or IP address of the proxy system with this property.</td>
</tr>
<tr>
<td>tw.server.host</td>
<td>The IP address or FQDN of your TE Server.</td>
</tr>
<tr>
<td>tw.server.port</td>
<td>The port on your TE Server that receives inbound communications from Agents (default = 9898).</td>
</tr>
<tr>
<td>webserver.http.port</td>
<td>If your TE Server is using a port other than 8080 to download JAR files to TE Agent systems, enter the port that is in use by the TE Server.</td>
</tr>
</tbody>
</table>
Step 3. Configuring TE Agents for Communication with the Proxy

You can configure a TE Agent system to work with your TE proxy either during or after installation of the system’s TE Agent software.

| Note | Axon Agents use a SOCK5 proxy instead of a TE proxy. To configure a proxy for Axon Agents, see Step 4. Configuring Axon Agent on page 90. |

To configure an existing TE Agent system to communicate with the TE proxy:

1. Open the Agent’s configuration file:
   <te_root>/agent/data/config/agent.properties

2. For the tw.proxy.host property, enter the IP address or FQDN of the TE proxy.

3. If you entered a non-default port for the tw.proxy.serverPort on the TE proxy (see Table 34 on the previous page), enter the same port number for the tw.proxy.port property.

4. Make sure that the tw.server.host property uses the correct IP address or FQDN.

To configure a TE Agent system at the time of installation, complete the appropriate installation procedure in Chapter 2: Installing Tripwire Enterprise Agent (on page 39).

- To launch the installer for a silent installation on an AIX or Linux system, the installer-launch command must also include the command-line components defined in Table 35 below.

- In the installer’s TE Server Hostname field, enter the FQDN or IP address you specified in Step 1. Configuring Your Tripwire Enterprise Server (on page 117).

Table 35. Additional command-line components for silent installations of AIX, Linux, and Windows TE Agents

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command-Line Components for your TE Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX and Linux</td>
<td>To specify the FQDN or IP address of the TE proxy, enter: &lt;br&gt; --proxy-host &lt;proxy_host&gt; &lt;br&gt; (Optional) To specify the port for connections to the TE proxy, enter: &lt;br&gt; --proxy-port &lt;proxy_port&gt;</td>
</tr>
<tr>
<td>Windows</td>
<td>To specify the FQDN or IP address of the TE proxy, enter: &lt;br&gt; TE_PROXY_HOSTNAME=&lt;host&gt; &lt;br&gt; (Optional) To specify the port for connections to the TE proxy, enter: &lt;br&gt; TE_PROXY_PORT=&lt;port&gt;</td>
</tr>
</tbody>
</table>
Step 4. Configuring the Firewall

To enable your TE Server to successfully communicate with a configured TE Agent via your TE proxy, you must configure the firewall that separates the TE Server from the TE Agent.

To configure your firewall:

- Enable traffic from the TE proxy to the TE Server on port 8080 and the Agent-communication port (tw.local.port).

- Enable traffic from the TE Server to the TE proxy on the port defined by the tw.proxy.serverPort property (see Table 34 on page 118) and the Agent-communication port (tw.local.port).
Chapter 5. Maintenance Procedures
Maintenance of Tripwire Enterprise

To configure Tripwire Enterprise, see the Tripwire Enterprise User Guide. Following configuration, your Tripwire Enterprise Administrator should regularly complete the procedures listed in Table 36 to maintain the integrity and operational efficiency of your Tripwire Enterprise implementation. Table 36 briefly describes each of these tasks and identifies the frequency with which each procedure should be completed.

Table 36. Maintenance procedures for Tripwire Enterprise

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Complete this procedure ...</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archiving log messages</td>
<td>... at least once per week</td>
<td>Created by default when Tripwire Enterprise is installed, the Archive Log Messages Task exports specified log messages to an XML file. For instructions on running and scheduling this task, see How Does the Archive Log Messages Task Work? in the Tripwire Enterprise User Guide.</td>
</tr>
<tr>
<td>Backing up Tripwire Enterprise data</td>
<td>... once per day (after all of the day’s report tasks have run)</td>
<td>To create backup files of your Tripwire Enterprise database and configuration files, see Backing Up Tripwire Enterprise Data and Configuration Files on the next page.</td>
</tr>
<tr>
<td>Regenerating database indices</td>
<td>... at least once per month*</td>
<td>To optimize system efficiency and speed, update the indices for your Tripwire Enterprise Console database by running the regeneration utility. For instructions, see Recalculating Database-Index Statistics on page 142.</td>
</tr>
</tbody>
</table>

* Any time you delete a large number of elements, nodes, and/or rules, you should regenerate your database indices.
Backing Up and Restoring Tripwire Enterprise

Backing Up Tripwire Enterprise Data and Configuration Files

To safeguard your Tripwire Enterprise implementation from data loss or corruption, you should back up the data in your TE database on a regular basis.

In addition to data files, you should also regularly create backup copies of your Tripwire Enterprise configuration files. With these files, you can restore a compromised TE Console installation or migrate an existing installation to a new system.

To create backups of your Tripwire Enterprise data and configuration files:

1. At a command prompt on your Tripwire Enterprise Server, enter the following command to stop the Tripwire Enterprise Console services.

   `<te_root>/server/bin/twservices stop`

2. To back up data files, see the documentation provided by the database vendor.

   **Note** To back up the data on a legacy MySQL database that was installed with Tripwire Enterprise 8.3 or earlier, see the *Tripwire Enterprise Installation & Maintenance Guide* for the version of TE used to install the database.

To back up TE configuration files, enter the following command at a command prompt on your Tripwire Enterprise Server:

   `<te_root>/server/bin/tetool backup <config_file>`

For command-line variable descriptions, see Table 37 on the next page. To specify the maximum size of each backup file, add the `--split` command:

   `--split <file_size>`

3. To restart the Tripwire Enterprise Console services, enter the following command:

   `<te_root>/server/bin/twservices start`

   **Tip** To verify the integrity of backed up files, we recommend that you use the files to restore a test system (see *Restoring Tripwire Enterprise Data and Configuration Files* on page 125).
Table 37. Backup command line variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;te_root&gt;</code></td>
<td>The installation directory for Tripwire Enterprise Console.</td>
</tr>
</tbody>
</table>
| `<config_file>` | The name of your configuration backup files. The `tetool` utility uses this value to name the first configuration backup file created. If your Tripwire Enterprise configuration files exceed the size specified by the `<file_size>` variable, `tetool` creates additional configuration backup files with an incremental, 3-digit extension. For example, if you enter `config.bak` as the file name, `tetool` would assign the following names to the backup files:  
  - `config.bak` (backup file #1)  
  - `config.bak.001` (backup file #2)  
  - `config.bak.002` (backup file #3)  
  - etc.  
  
  **Note:** The `<config_file>` variable can include an absolute or relative path. |
| `<file_size>` | (Optional) The maximum size of each backup file. For example, if your Tripwire Enterprise data totals 7GB, and you enter 3GB as the file size, `tetool` will create three data backup files; two 3GB files, and one 1GB file.  
  When entering the file size, use the `--split` command with the following abbreviations:  
  - G or g = gigabytes  
  - M or m = megabytes  
  - K or k = kilobytes  
  For example, `--split=640M` or `--split=640m`. |
Restoring Tripwire Enterprise Data and Configuration Files

If you created backup files for your Tripwire Enterprise data or configuration files (see Backing Up Tripwire Enterprise Data and Configuration Files on page 123), use the procedure in this section to restore them.

**Note** You can only restore Tripwire Enterprise Console using a backup file created from the same version of the TE Console software.

To restore your Tripwire Enterprise data or configuration files, complete the following steps:

*Step 1. Import Backup Files to the Tripwire Enterprise Server (below)*

*Step 2. Restart Tripwire Enterprise Agents (on the next page)*

### Step 1. Import Backup Files to the Tripwire Enterprise Server

To import your backup files:

1. At a command prompt on your Tripwire Enterprise Server, enter the following command to stop the Tripwire Enterprise Console services.

   `<te_root>/server/bin/twservices stop`

2. To restore data files, see the documentation provided by your database vendor.

   **Note** To restore data files on a legacy MySQL database that was installed with Tripwire Enterprise 8.3 or earlier, see the Tripwire Enterprise Installation & Maintenance Guide for the version of TE used to install the database.

To restore TE configuration files, enter:

`<te_root>/server/bin/tetool restore <config_file>`

For command-line variable definitions and guidelines, see Table 38 on the next page.

**Caution** To restore a Tripwire Enterprise Server with a hostname that differs from the hostname of the server on which the backup files were created, you must add the --safe option to the command. Otherwise, the restored system may suffer unrecoverable errors on startup. (With the --safe option, Tripwire Enterprise only restores essential files.)

3. To register the local TE Agent with the restored Console, enter:

   `<te_root>/server/bin/tetool create-agent-key-store <hostname>`

   and follow the directions.

4. To restart the Tripwire Enterprise Console services, enter the appropriate command.

   `<te_root>/server/bin/twservices start`
Table 38. Restore command line variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;te_root&gt;</td>
<td>The installation directory for Tripwire Enterprise Console.</td>
</tr>
<tr>
<td>&lt;config_file&gt;</td>
<td>The name of the first configuration backup file.</td>
</tr>
</tbody>
</table>

*Note:* For information about the naming scheme employed for configuration and data backup files, see Table 37 on page 124.

---

**Step 2. Restart Tripwire Enterprise Agents**

Once your backup files have been imported (*Step 1. Import Backup Files to the Tripwire Enterprise Server on the previous page*), all Tripwire Enterprise Agents must be restarted and refreshed. Data refresh synchronizes the local TE Agent databases with your Tripwire Enterprise Console database.

**Caution**

When you restart a TE Agent that has an Event Generator, the Agent discards any pooled audit events and/or change versions.

Do not baseline or version check a TE Agent node while it is re-starting. When an Agent has been successfully restarted, Tripwire Enterprise will create the following System log message in the Log Manager:

```
Finished recreating data on <Agent_node>
```

**To restart TE Agents:**

1. Log in to the Tripwire Enterprise interface with the administrator account.
2. Click NODES.
3. Click *Modify* > *Restart Agents*.
4. In the confirmation dialog, click OK.
5. Select the *Refresh data on Agents* check box.
6. Click OK.

**Next** To update Tripwire Enterprise with the current state of the restarted TE Agents, run a version check on the Agent systems. For instructions, see *Version Checking Monitored Systems* in the *Tripwire Enterprise User Guide*. 
Updating Java for Tripwire Enterprise Console

This section describes the process to update the Java Runtime Environment (JRE) and Java Cryptography Extension (JCE) files used by Tripwire Enterprise Console. Both sets of files must be updated at the same time.

**To upgrade the JRE and JCE files on a TE Console system:**

1. Download the following files:
   - The Java SE 1.8 64-bit JRE installer for your platform
   - The JCE Unlimited Strength Jurisdiction Policy Files

   **Note** The TE Console Release Notes will list the latest JRE version that is supported for that version of Tripwire Enterprise. Upgrading to a newer version may work, but may also result in unexpected behavior.

2. Extract and run the JRE installer on the system where TE Console is installed.

   **Caution** At the end of the JRE installation, if you are prompted to remove obsolete versions, **DO NOT** do so.

3. Extract and install the JCE Policy Files on the TE Console system:
   a. Extract the JCE files.
   b. Copy the `local_policy.jar` and `US_export_policy.jar` files from the JCE to the new JRE's `/lib/security` directory, overwriting the existing files.

4. Update the `TW_JAVA_HOME` environment variable to point to the new JRE.

   **For TE Consoles installed on Windows:**
   a. Open the Windows Control Panel.
   b. Type `environment` into the Search box, then click **Edit the system environment variables** in the search results dialog.
   c. In the System Properties dialog, click the **Environment Variables** button.
   d. In the Environment Variables dialog, scroll through the **System variables** list and double-click **TW_JAVA_HOME**.
   e. Edit the **Variable value** to point to the new JRE directory, then click **OK**.
   f. In the Environment Variables dialog, scroll through the **User variables** list and double-click **TW_JAVA_HOME**.
   g. Edit the **Variable value** to point to the new JRE directory, then click **OK**.
   h. Click **OK** to close all remaining dialogs.
For TE Consoles installed on Linux:

a. Obtain root privileges on the TE Console system.

b. Run the following command:

```bash
find ~ -maxdepth 1 -type f -name '.*' -exec grep -l 'TW_JAVA_HOME' {} \;
```

- print | sort | uniq

c. Open each listed file in a text editor and update TW_JAVA_HOME to point to the new JRE directory.

d. Update the TW_JAVA_HOME environment variable to point to the new JRE directory.

5. Open `<te_root>/server/bin/server.conf` in a text editor and set set.default.TW_JAVA_HOME to the new JRE directory.

6. Open `<te_root>/server/data/config/twjavahome` in a text editor and set the path to the new JRE directory.

7. From the command line, restart TE Console:

```bash
<te_root>/server/bin/twserver restart
```

8. Review the `<te_root>/server/data/teserver.log` file to confirm that TE Console is using the new JRE. The log record begins with "Using Java version...".

9. Open TE Console in your browser, and confirm that you can log in successfully.

10. After verifying that TE Console is operational, you can uninstall the old version of Java.
Changing the Console Used to Manage an Agent

After a TE Agent or Axon Agent has successfully connected to a TE Console, several steps are required to change the Console used to manage that Agent. This change may be required if you migrate your TE Console installation to a system with a different hostname, or for installations with multiple TE Consoles.

The process to change the managing TE Console is different for TE Agents and Axon Agents. For more information, see:

- *Changing the TE Console Used to Manage a TE Agent* (below)
- *Changing the TE Console Used to Manage an Axon Agent* (on the next page)

**Changing the TE Console Used to Manage a TE Agent**

To change the Tripwire Enterprise Console system used to manage a TE Agent:

1. On the TE Agent system, stop the TE Agent service as described in *Managing the Tripwire Enterprise Agent Service* on page 134.

2. Edit the Agent's `<te_root>/agent/data/config/agent.properties` file to change the `tw.server.host` value to the new Console’s hostname or IP address.

3. If the services passphrase on the new Console is different from the passphrase on the old Console, execute one of the following commands:

   **Windows:**
   ```
   <te_root>\Agent\bin\tetool.cmd setchannelpass "<old_services_passphrase>" "<new_services_passphrase>"
   ```

   **UNIX:**
   ```
   <te_root>/agent/bin/tetool setchannelpass '<old_services_passphrase>' '<new_services_passphrase>'
   ```


5. If the Agent is older than TE 8.4.1 and uses FIPS mode, delete the `<te_root>/agent/data/security/security.csp` file.

6. Start the TE Agent service as described in *Managing the Tripwire Enterprise Agent Service* on page 134.
Changing the TE Console Used to Manage an Axon Agent

To change the TE Console used to manage an Axon Agent:

1. Complete the following steps on the new Tripwire Enterprise Server:
   a. If needed, upgrade to the latest version of Tripwire Enterprise Console.
   b. Configure the Bridge, as described in Step 1. Configuring the Axon Bridge on page 83.

2. Complete the following steps on the Axon Agent host system:
   a. Shut down the Tripwire Axon Agent service by entering one of the following commands:
      
      **Linux (RHEL and CentOS):** /sbin/service tripwire-axon-agent stop
      **Linux (Debian and Ubuntu):** /usr/sbin/service tripwire-axon-agent stop
      **Windows:** net stop TripwireAxonAgent
   b. Delete the following certificates.
      
      **Linux:** /var/cache/tripwire/trust/keystore.p12
      **Windows:** %PROGRAMDATA%\Tripwire\agent\data\trust\keystore.p12
   c. Open the Axon Agent configuration file (twagent.conf) in the appropriate directory.
      
      **Linux:** /etc/tripwire/
      **Windows:** %PROGRAMDATA%\Tripwire\agent\config\n   d. In the configuration file, enter the IP address or host name of the new Tripwire Enterprise Server as the bridge.host option, and edit the other options, as needed (see Table 23 on page 92).
   e. Create a text file named registration_pre_shared_key.txt and save the file in the following directory:
      
      **Linux:** /etc/tripwire/
      **Windows:** %PROGRAMDATA%\Tripwire\agent\config\n   f. In the text file, enter the registration pre-shared key (value only) for the new Agent Bridge.
   g. Start the Tripwire Axon Agent service by entering one of the following commands at a command prompt.
      
      **Linux (RHEL and CentOS):** /sbin/service tripwire-axon-agent start
      **Linux (Debian and Ubuntu):** /usr/sbin/service tripwire-axon-agent start
      **Windows:** net start TripwireAxonAgent
Changing the Services and Database Passphrases

Changing the Tripwire Enterprise Services Passphrase

The services passphrase establishes initial trust between the Tripwire Enterprise Console and Tripwire Enterprise Agent software. The services passphrase is first specified when TE Console is installed. In order to change the services passphrase, you must execute commands on both the system where the TE Console is installed, and on each system where TE Agent is installed.

The services passphrase must be between 19 and 64 characters. Most ASCII printable characters are allowed, with a few exceptions:

- Alphanumeric characters (a-z, A-Z, 0-9), the space character (ASCII decimal 32), and most punctuation characters (\-!@#$%^&*(),_+={}|?/:;\) are allowed.
- The single-quote ('), double-quote ("), less-than (<), greater-than (>) and backslash (\) characters are not allowed.

To change the services passphrase:

1. Execute one of the following commands on the TE Console system:
   - Windows: \Server\bin\tetool.cmd setchannelpass "<services_passphrase>" "<new_services_passphrase>"
   - UNIX: \server/bin/tetool setchannelpass '<services_passphrase>' '<new_services_passphrase>'

2. Restart the TE Console services:
   - \Server\bin\twservices restart

3. Execute one of the following commands on each system where TE Agent software is installed:
   - Windows: \Agent\bin\tetool.cmd setchannelpass "<old_services_passphrase>" "<new_services_passphrase>"
   - UNIX: \agent/bin/tetool setchannelpass '<old_services_passphrase>' '<new_services_passphrase>'

4. Restart the TE Agent services on each Agent system, as described in Managing the Tripwire Enterprise Agent Service on page 134.
Changing the Tripwire Enterprise Database Passphrase

The database passphrase secures communication between the Tripwire Enterprise Console and a remote database. The database passphrase is first specified when the remote database is initially created. In order to change the database passphrase, you must execute commands on both the system where the TE Console is installed, and on the system where the database is installed.

The database passphrase must be between 6 and 64 characters. Most ASCII printable characters are allowed, with a few exceptions:

- Alphanumeric characters (a-z, A-Z, 0-9), the space character (ASCII decimal 32), and most punctuation (_`^-!@#$%^&*(),.+*[]{}|:/?) are allowed.
- The single-quote ('), double-quote ('"), less-than ('<'), greater-than ('>'), and backslash ('\') characters are not allowed.

To change the database passphrase:

1. Stop the TE Console services:
   ```bash
   <te_root>\server\bin\twservices stop
   ```

2. Change the passphrase on the remote database. See your database documentation for specific instructions on changing this passphrase.

3. Execute one of the following commands on the TE Console system:
   ```bash
   Windows: <te_root>\Server\bin\tetool.cmd setdatabasepass "<services_passphrase>" "<new_database_passphrase>"
   UNIX: <te_root>/server/bin/tetool setdatabasepass '<services_passphrase>' '<new_database_passphrase>'
   ```
   Make sure that new_database_passphrase exactly matches the passphrase you specified for the remote database.

4. Restart the TE Console services:
   ```bash
   <te_root>\server\bin\twservices restart
   ```
Managing Tripwire Enterprise Services

Managing Tripwire Enterprise Console Services

Tripwire Enterprise Console services are processes that monitor the systems on your network, generate Tripwire Enterprise (TE) data, and transfer data between your Tripwire Enterprise Server and TE interface sessions. Once Tripwire Enterprise Console software is installed, these services run continually by default. To start, stop, or check TE Console services, enter the appropriate command at a command prompt on your TE Server (see Table 39).

<table>
<thead>
<tr>
<th>Caution</th>
<th>Tripwire Enterprise Console services provide continuous monitoring of your network. Therefore, services should not be stopped unless you need to backup TE data, restore data from backup, upgrade the software, or run a tetool command.</th>
</tr>
</thead>
</table>
| Notes | You can also start, stop, or check Tripwire Enterprise Console services from the Windows Start menu on your TE Server.  
<te_root> is the installation directory for Tripwire Enterprise Console software. |

Table 39. Commands for Tripwire Enterprise Console services

<table>
<thead>
<tr>
<th>Function</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>&lt;te_root&gt;\Server\bin\twservices start</td>
</tr>
<tr>
<td>Stop</td>
<td>&lt;te_root&gt;\Server\bin\twservices stop</td>
</tr>
<tr>
<td>Check</td>
<td>&lt;te_root&gt;\Server\bin\twservices check</td>
</tr>
<tr>
<td>Note: This command verifies that Tripwire Enterprise Console services are running.</td>
<td></td>
</tr>
<tr>
<td>Restart</td>
<td>&lt;te_root&gt;\Server\bin\twservices restart</td>
</tr>
</tbody>
</table>
Managing the Tripwire Enterprise Agent Service

The Tripwire Enterprise Agent service is a process that runs on a monitored file server. The Agent service collects change data for the file server, and reports this data to the Tripwire Enterprise Server.

When an Agent is installed on a file server, the Agent service runs continually by default. To start, stop, or check the Tripwire Enterprise Agent service, enter the appropriate command(s) at a command prompt on the Agent host system (see Table 40 below).

<table>
<thead>
<tr>
<th>Notes</th>
<th>On Windows systems, you can also start, stop, or check Agent services from the Windows Start menu on the Agent host system.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>On OS X systems, you can also start or stop Agent services from the <strong>Applications &gt; Utilities &gt; Services</strong> section of the UI on the Agent host system.</td>
</tr>
<tr>
<td></td>
<td>Administrator or root privileges are required to run these commands.</td>
</tr>
<tr>
<td></td>
<td>&lt;te_root&gt; is the installation directory for Tripwire Enterprise Agent software.</td>
</tr>
</tbody>
</table>

Table 40. Commands for Tripwire Enterprise Agent services

<table>
<thead>
<tr>
<th>Function</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start</strong></td>
<td>On an <strong>AIX</strong> system, run these commands to start the TE Agent and its services:</td>
</tr>
<tr>
<td></td>
<td><code>startsrc -s teges</code></td>
</tr>
<tr>
<td></td>
<td><code>startsrc -s teeg</code></td>
</tr>
<tr>
<td></td>
<td><code>startsrc -s tteagent</code></td>
</tr>
<tr>
<td></td>
<td>On an <strong>OS X</strong> system: <code>launchctl start com.tripwire.te.agent</code></td>
</tr>
<tr>
<td></td>
<td>On a <strong>Solaris</strong> system: <code>$ svcadm enable teagent</code></td>
</tr>
<tr>
<td></td>
<td>On other <strong>UNIX or Linux</strong> systems: <code>&lt;te_root&gt;/agent/bin/twdaemon start</code></td>
</tr>
<tr>
<td></td>
<td>On a <strong>Windows</strong> system: <code>&quot;&lt;te_root&gt;\Agent\bin\twdaemon&quot; start</code></td>
</tr>
<tr>
<td><strong>Stop</strong></td>
<td>On an <strong>AIX</strong> system, run these commands to stop the TE Agent and its services:</td>
</tr>
<tr>
<td></td>
<td><code>stopsrc -s tteagent</code></td>
</tr>
<tr>
<td></td>
<td><code>stopsrc -s teeg</code></td>
</tr>
<tr>
<td></td>
<td><code>stopsrc -s tege</code></td>
</tr>
<tr>
<td></td>
<td>On an <strong>OS X</strong> system: <code>launchctl stop com.tripwire.te.agent</code></td>
</tr>
<tr>
<td></td>
<td>On a <strong>Solaris</strong> system: <code>$ svcadm disable teagent</code></td>
</tr>
<tr>
<td></td>
<td>On other <strong>UNIX or Linux</strong> systems: <code>&lt;te_root&gt;/agent/bin/twdaemon stop</code></td>
</tr>
<tr>
<td></td>
<td>On a <strong>Windows</strong> system: <code>&quot;&lt;te_root&gt;\Agent\bin\twdaemon&quot; stop</code></td>
</tr>
<tr>
<td>Function</td>
<td>Commands</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| **Check** | On an **AIX 5.3 or higher** system: $ lssrc -a  
On a **Solaris** system: $ svcs -a | grep tripwire  
On other **UNIX or Linux** systems: `<te_root>/agent/bin/twdaemon` status  
On a **Windows** system: "<te_root>\Agent\bin\twdaemon" status |
| **Restart** | On a **Solaris** system: $ svcadm restart teagent  
On other **UNIX or Linux** systems: `<te_root>/agent/bin/twdaemon` restart  
On a **Windows** system: "<te_root>\Agent\bin\twdaemon" restart |

**Note:** These commands verify that Tripwire Enterprise Agent services are running. For Solaris, the command generates a list of active subsystems or services. If 'teagent' appears in the list with the state 'online' for Solaris, the Agent is running.
Managing the Axon Agent Service

The Axon Agent service is a process that runs on a monitored file server that has Axon Agent installed. The Axon Agent service collects change data for the file server, and reports this data to a Tripwire Enterprise Console.

When an Axon Agent is installed on a file server, the Axon Agent service runs continually by default. To start or stop the Axon Agent service, enter the appropriate command at a command prompt on the Agent host system (see Table 41 below).

| Note | Administrator or root privileges are required to run these commands. |

**Table 41. Commands for Axon Agent services**

<table>
<thead>
<tr>
<th>Function</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start</strong></td>
<td>On a Linux (RHEL or CentOS) system: /sbin/service tripwire-axon-agent start&lt;br&gt;On a Linux (Debian or Ubuntu) system: /usr/sbin/service tripwire-axon-agent start&lt;br&gt;On a Windows system: net start TripwireAxonAgent</td>
</tr>
<tr>
<td><strong>Stop</strong></td>
<td>On a Linux (RHEL or CentOS) system: /sbin/service tripwire-axon-agent stop&lt;br&gt;On a Linux (Debian or Ubuntu) system: /usr/sbin/service tripwire-axon-agent stop&lt;br&gt;On a Windows system: net stop TripwireAxonAgent</td>
</tr>
</tbody>
</table>
Managing the Event Generator Service

When installing TE Agent software on a supported Windows or Linux system, you have the option of installing an Event Generator at the same time. When installing Axon Agent, the Event Generator is either installed automatically (on Windows systems) or must be installed separately (on Linux systems). If you don't install the Event Generator with the Agent software, you can also install it at a later time.

If an Event Generator is installed on a system, audit event collection (but not real-time monitoring) is enabled automatically for that node and the Event Generator is used as the source for audit events. For more information, see *What is Audit Event Collection? and How Does Real-Time Monitoring Work?* in the *Tripwire Enterprise User Guide*

For a complete list of operating systems on which the Event Generator can be installed, see:

http://www.tripwire.com/register/tripwire-enterprise-platform-and-device-support

To install, uninstall, start, stop, or check the status of an Event Generator, enter the appropriate command at a command prompt on the Agent system:

- Table 42 (on the next page) lists commands for TE Agent systems
- Table 43 (on page 139) lists commands for Axon Agent systems

| Notes | To resume the collection of audit events following a restart of an Event Generator on a TE Agent system, you must restart and refresh the TE Agent. For instructions, see *Step 2. Restart Tripwire Enterprise Agents on page 126*. This step is not necessary on Axon Agent systems.

On OS X systems, you can also start and stop the Event Generator service from the Applications > Utilities > Services section of the UI on the Agent host system.

On Windows systems, you can also start, stop, restart, and view the status of the Event Generator service from the Services dialog. To launch this dialog, enter services.msc at a command prompt.

<te_root> is the installation directory for Tripwire Enterprise Console or Tripwire Enterprise Agent software. |
Table 42. Commands for Event Generators on TE Agent systems

<table>
<thead>
<tr>
<th>Function</th>
<th>Commands</th>
</tr>
</thead>
</table>
| Install  | On a **Linux** TE Agent: `<te_root>/bin/twrtmd installrtm`  
|          | On a **Windows** TE Agent: `"<te_root>/bin\twdaemon" installrtm`  |
| Restart  | On a **Linux** TE Agent: `/etc/init.d/twrtmd restart`  
|          | On a **Solaris** TE Agent: `$ svcadm restart teeg`  |
| Start    | On an **AIX** system, run these commands to start the Event Generator:  
|          | `startsrc -s teges`  
|          | `startsrc -s teeg`  
|          | On a **Linux** TE Agent: `/etc/init.d/twrtmd start`  
|          | On an **OS X** TE Agent: `launchctl start com.tripwire.te.tesvc`  
|          | On a **Solaris** TE Agent: `$ svcadm enable teeg`  
|          | On a **Windows** TE Agent: `"<te_root>/bin\twdaemon" startrtm`  |
| Status   | On a **Linux** TE Agent: `/etc/init.d/twrtmd status`  
|          | On a **Solaris** TE Agent: `$ svcs -a | grep tripwire`  
|          | On a **Windows** TE Agent: `"<te_root>/bin\twdaemon" status`  
|          | **Note:** These commands verify that the Event Generator is running. For Solaris, if `teeg` appears in the list with the state 'online,' the Event Generator is running.  |
| Stop     | On an **AIX** system, run these commands to stop the Event Generator:  
|          | `stopsrc -s teges`  
|          | `stopsrc -s teeg`  
|          | On a **Linux** TE Agent: `/etc/init.d/twrtmd stop`  
|          | On an **OS X** TE Agent: `launchctl stop com.tripwire.te.tesvc`  
|          | On a **Solaris** TE Agent: `$ svcadm disable teeg`  
|          | On a **Windows** TE Agent: `"<te_root>/bin\twdaemon" stoprtm`  |
| Uninstall| On a **Linux** TE Agent: `/etc/init.d/twrtmd uninstallrtm`  
|          | On a **Windows** TE Agent: `"<te_root>/bin\twdaemon" uninstallrtm`  
|          | **Note:** The Linux command removes the Event Generator daemon and activates bypass mode for the kernel module. To permanently remove the kernel module, re-boot the system.  |
Table 43. Commands for Event Generators on Axon Agent systems

<table>
<thead>
<tr>
<th>Function</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Install</strong></td>
<td>For Event Generator installation commands and instructions, see <em>Step 3. Installing Axon Agent Software on page 86</em>.</td>
</tr>
</tbody>
</table>
| **Restart** | On a **Linux** Axon Agent: service tw-eg-service restart  
On a **Windows** Axon Agent: net stop TripwireEventGeneratorService & net start TripwireEventGeneratorService |
| **Start** | On a **Linux** Axon Agent: service tw-eg-service start  
On a **Windows** Axon Agent: net start TripwireEventGeneratorService |
| **Status** | On a **Linux** Axon Agent: service tw-eg-service status  
On a **Windows** Axon Agent: sc query TripwireEventGeneratorService |
| **Stop** | On a **Linux** Axon Agent: service tw-eg-service stop  
On a **Windows** Axon Agent: net stop TripwireEventGeneratorService |
| **Uninstall** | On a **Linux** Axon Agent: See *Uninstalling Axon Agent on page 101*.  
On a **Windows** Axon Agent: The Event Generator is uninstalled automatically when Axon Agent is uninstalled, and cannot be removed independently. |
Managing TE Services with the Solaris Service Management Facility

A feature of some Solaris operating systems, the Service Management Facility (SMF) simplifies the management of hosted services. If a Tripwire Enterprise Agent is installed on a Solaris system with the SMF, you can control the following TE services from the system's command line (see Table 44 below):

- Global Event Source (teges)
- Event Generator (teeg)
- Tripwire Enterprise Agent (teagent)

Table 44. Commands to manage TE services with the Solaris Service Management Facility

<table>
<thead>
<tr>
<th>Function</th>
<th>Commands</th>
</tr>
</thead>
</table>
| **Start** | To start one or more TE services, enter:  
  $ svcadm enable <services>  
  Where <services> is the name of each service to be started. For example, to start the Global Event Source, Event Generator, and Tripwire Enterprise Agent services, enter:  
  $ svcadm enable teges teeg teagent  
  **Note:** The Global Event Source (teges) only exists in global zones on a Solaris system. |
| **Stop** | To stop a single TE service, enter:  
  $ svcadm disable <service>  
  Where <service> is the name of the service to be stopped. |
| **Restart** | To restart a single TE service, enter:  
  $ svcadm restart <service>  
  Where <service> is the name of the service to be restarted. |
| **List** | To generate a list of the TE services in SMF, enter:  
  $ svcs -a | grep tripwire |
Managing the Tripwire Enterprise Console Database

About Database Maintenance

You can mitigate the growth of your Tripwire Enterprise Console database by periodically running the following Tripwire Enterprise tasks:

- The **Archive Log Messages Task** archives all Tripwire Enterprise log messages that exceed a specified age or number. For more information, see *How Does the Archive Log Messages Task Work?* in the *Tripwire Enterprise User Guide*.

- The **Compact Element Versions Task** removes all content and attributes from element versions that exceed a specified age or number. For more information, see *How Does the Compact Element Versions Task Work?* in the *Tripwire Enterprise User Guide*.

Each of these tasks reduces the quantity of data stored in your Tripwire Enterprise Console database (unless the database is a MySQL database).

A **database index** is a data structure that improves the speed of operations in a database table. Like the index of a book, a database index contains entries that reference specific information in the database. A **query optimizer** is a database component that uses database-index statistics to determine the most efficient way to execute a query.

**To optimize system efficiency and speed, you should recalculate the database-index statistics for your Tripwire Enterprise Console database on a weekly basis.** To recalculate statistics, Tripwire Enterprise refreshes the database indices with the latest information in the Tripwire Enterprise Console database. For instructions, see *Recalculating Database-Index Statistics* on the next page.
Recalculating Database-Index Statistics

For an introduction to database indices, see *About Database Maintenance* on the previous page.

**Caution**  Recalculating database-index statistics may take several hours, depending on the size of the database. No user activity will be possible during this time, and you should ensure that no tasks are scheduled to run at this time.

To recalculate index statistics for your Tripwire Enterprise Console database:

1. Click SETTINGS.
2. Under the System folder, click Database.
4. Click Apply.
5. In the confirmation dialog, click OK.
**Index**

A

admin file
  creating for Solaris TE Agent installation 65

Agent update packs
  installing for upgrade of Tripwire Enterprise Agent 77

AIX
  additional requirements for TE Agent 43
  installing Tripwire Enterprise Agent on 44
  interactive installation of TE Agent 44
  restoring audit configuration files 48
  silent installation of TE Agent 46

Apple OS X
  installing Tripwire Enterprise Agent on 49
  interactive installation of TE Agent 49
  silent installation of TE Agent 51

Axon Agent
  assigning tags with tag files 96
  authentication 81
  changing the TE Console for 106, 130
  configuration file options 90
  configuring a DNS SRV record 85
  configuring TLS versions 103
  creating a support bundle 112
  determining version 102
  error messages 110
  installing 83
  installing silently 94
  managing services 136
  ports and services 82
  revoking certificates 107
  supported platforms 81
  troubleshooting 108
  uninstalling 101
  upgrading 98
Axon Bridge
  configuring 83
  configuring TLS versions 103
  defined 81

B

backing up
  Tripwire Enterprise data 123

C

configuring
  a firewall for a TE proxy 120
  a remote Microsoft SQL Server database 17
  a remote MySQL database 15
  a remote Oracle database 16
  a TE proxy for TE Agent communication 117
  a TE Server for use with a TE proxy 117
  a Tripwire Enterprise Server for use with Multiple NICs 116
  TE Agents for communication with a TE proxy 119
  Tripwire Enterprise Agent for use with Multiple NICs 116
  Tripwire Enterprise inside a Network Address Translation (NAT) environment 114

D

database-index statistics
  recalculating 142

database indices
  about 141
  recalculating statistics for 142

database passphrase
  changing 132
  setting 14

DKMS
  using with Axon Agent 88, 99-100

DNS SRV records
  configuring for an Axon Agent 85
error messages
   for the Axon Agent 110

EULA
   for Tripwire Enterprise Agent 40

Event Generator
   installing with Axon Agent 87, 89
   using DKMS 88, 99-100

Event Generators
   managing services 137

FIPS mode
   See the Tripwire Enterprise Hardening Guide

firewalls
   configuring for use with a TE proxy 120

Global Event Source
   configuring for non-global zones on Solaris 63

HP-UX
   additional requirements for TE Agent 43
   installing Tripwire Enterprise Agent on 53
   interactive installation of Agent 53
   silent installation of TE Agent 55

installing
   a remote database 14
   a TE proxy 118
   Axon Agent 83
   Java for a new TE Console installation 26
installing Tripwire Enterprise Agent
  on AIX 44
  on Apple OS X 49
  on HP-UX 53
  on Linux 57
  on Solaris 61
  on Windows 67
  preparation 41
  requirements 40

installing Tripwire Enterprise Console
  new installations 25
  requirements for a new installation 25
  requirements for an upgrade 33
  upgrade installations 33

interactive installation
  defined 40

J

Java
  installing for a new TE Console installation 26
  updating for TE Console 127

L

Linux
  installing Tripwire Enterprise Agent on 57
  interactive installation of TE Agent 57
  silent installation of TE Agent 59

M

maintenance
  of Tripwire Enterprise 122
  of Tripwire Enterprise Console database 141

managing
  Axon Agent services 136
  Tripwire Enterprise Agent services 134
  Tripwire Enterprise Console databases 141
Tripwire Enterprise Console services 133
Tripwire Enterprise Event Generators 137
Tripwire Enterprise services with the Solaris Service Management Facility 140

MySQL
  configuring a remote database for TE Console 15

N

NAT
  using with Tripwire Enterprise 114

Network Address Translation
  see NAT 114

network requirements
  for Tripwire Enterprise Agent 43

NIC
  configuring a Tripwire Enterprise Server for use with multiple NICs 116
  configuring Tripwire Enterprise Agents for use with multiple NICs 116

O

Oracle
  configuring a remote database for TE Console 16

P

passphrases
  changing the database passphrase 132
  changing the services passphrase 131
  setting the database passphrase 14

platforms
  supported by Tripwire Enterprise Agent 43

ports
  default ports for a remote database server 14
  optional outbound ports for a Tripwire Enterprise Server 31
  required for a Tripwire Enterprise Server 31
  requirements for Tripwire Enterprise Agent 43
  used by the Axon Agent 82
pre-shared key
defined 81

properties
for a TE proxy system 118

R

remote database servers
requirements for 14

remote databases
changing the passphrase for 132
configuring a remote Microsoft SQL Server database 17
configuring a remote MySQL database 15
configuring a remote Oracle database 16
installing 14

requirements
for a remote database server 14
for new TE Console installations 25
for Tripwire Enterprise Agent 43
for upgrading TE Console 33

restarting
TE Agents during a TE Console upgrade 35

restoring
Tripwire Enterprise data 125

S

services
installed with the Axon Agent 82
installed with Tripwire Enterprise Agent 42
installed with Tripwire Enterprise Console 30
managing for Axon Agent 136
managing for TE Agent 134

services passphrase
changing 131

silent installation
defined 40
Solaris
  additional requirements for TE Agent 43
  configuring the Global Event Source for non-global zones 63
  installing Tripwire Enterprise Agent on 61
  interactive installation of TE Agent 61
  silent installation of TE Agent 64
Solaris Service Management Facility
  managing TE services with 140
SQL Server
  configuring a remote database for TE Console 17
support bundle
  creating for an Axon Agent 112

tag files
  using with Axon Agents 96
  using with TE Agents 72
tags
  assigning to new Axon Agents with tag files 96
  assigning to new TE Agents with tag files 72
TE proxies
  configuring for TE Agent communication 117
  installing 118
  properties 118
TLS
  configuring versions for Axon Agents 103
  configuring versions for TE Agents 74
  supported versions and cipher suites for Axon Agent 105
Tripwire Enterprise
  backing up Tripwire Enterprise data 123
  maintenance of 122
  restoring Tripwire Enterprise data 125
  using with NAT 114
Tripwire Enterprise Agent
  assigning tags with tag files 72
  changing the Console used to manage a TE Agent 129
  changing the services passphrase 131
configuring a TE proxy for 117
configuring for communication with a TE proxy 119
configuring for use with multiple NICs 116
configuring TLS versions 74
defined 40
EULA 40
installation requirements 40
installing on AIX 44
installing on Apple OS X 49
installing on HP-UX 53
installing on Linux 57
installing on Solaris 61
installing on Windows 67
interactive installation for AIX 44
interactive installation for Apple OS X 49
interactive installation for HP-UX 53
interactive installation for Linux 57
interactive installation for Solaris 61
interactive installation for Windows 67
managing services 134
network requirements 43
port requirements 43
preparing for installation 41
requirements for 43
restarting during a TE Console upgrade 35
services installed 42
silent installation for AIX 46
silent installation for Apple OS X 51
silent installation for HP-UX 55
silent installation for Linux 59
silent installation for Solaris 64
silent installation for Windows 69
supported platforms 43
uninstalling 79
upgrading software 78

Tripwire Enterprise Console
  changing the Console used to manage a TE Agent 129
  changing the Console used to manage an Axon Agent 106, 130
  changing the services passphrase 131
  configuring for use with multiple NICs 116
configuring TLS versions  74
managing services  133
requirements for a new installation  25
requirements for a remote database server  14
services installed  30
uninstalling  37
upgrade paths for older versions  36
upgrading  33

Tripwire Enterprise Console database
  about maintenance  141
  backing up data  123
  managing  141
  recalculating database-index statistics  142
  restoring data  125

Tripwire Enterprise proxies
  see TE proxies  117

Tripwire Enterprise Servers
  configuring for use with a TE proxy  117
  defined  13

troubleshooting
  Axon Agent  108

U

uninstalling
  Axon Agent  101
  Tripwire Enterprise Console  37
  Tripwire Enterprise Agent  79

upgrading TE Agents
  installing update packs  77
  upgrading software  78

upgrading TE Console
  after upgrading  35
  backing up data  33
  installing TE Console software  34
  requirements  33
  restarting TE Agents  35
  upgrade paths  36
Windows
  installing Tripwire Enterprise Agent on 67
  interactive installation of TE Agent 67
  silent installation of TE Agent 69