FORCEPOINT
POWERED BY Raytheon

TRITON® Manager Help

Forcepoint™ TRITON Solutions

v8.2.x

10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin TX 78759

Published 2016

Trademarks

Contents

1 Getting Started

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

TRITON Manager is a browser-based console that provides a central, graphical interface to the general configuration, policy management, and reporting functions of your security software.

TRITON Manager includes one or more of the following modules, depending on your subscription:

- **TRITON AP-WEB** or Web Filter & Security work in conjunction with integration devices (including proxy servers, firewalls, routers, and caching appliances) and enable you to develop, monitor, and enforce Internet access policies.
- **TRITON AP-DATA** protects organizations from information leaks and data loss both at the perimeter and inside the organization.
- **TRITON AP-EMAIL** protects your organization against the threats of malware, spam, and other unwanted content in email traffic.

If your subscription includes TRITON AP-MOBILE, TRITON Manager also provides a link to a cloud-based console used to manage threat protection and data loss prevention for mobile devices.

To learn to use TRITON Manager, browse this guide or select one of the following topics as a launch point.

First steps	Manage administrators
• *Logging on to TRITON Manager* • *Navigating in TRITON Manager* • *Managing your account through the My Account Portal* • *Viewing your account information*	• *Introducing administrators* • *Setting user directory information* • *Enabling access to TRITON Manager* • *Setting email notifications*
Other administrator tasks	**Backup and restore**
• *Configuring two-factor authentication* • *Audit log* • *Managing appliances*	• *Scheduling TRITON infrastructure backups* • *Restoring TRITON infrastructure backup data*

Logging on to TRITON Manager

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Related topics:

- *Logging on with RSA® SecurID authentication*, page 3
- *Logging on with certificate authentication*, page 4
- *Security certificate alerts*, page 5
- *TRITON Manager session time outs*, page 5

TRITON Manager is the central configuration interface used to manage software configuration and settings for your software modules. This Web-based tool runs on the following supported browsers:

- Microsoft Internet Explorer 8 - 9 (non-compatibility mode)
- Microsoft Internet Explorer 10 - 11 standard mode

> **Note**
> If you are using Internet Explorer, make sure Enhanced Security Configuration is switched off.

- Microsoft Edge 15, 20, and 25
- Mozilla Firefox 4.4 - 44
- Google Chrome 13 - 49

Although it is possible to launch TRITON Manager using some other browsers, use the supported browsers to receive full functionality and proper display of the application.

> **Note**
> Some animations in TRITON Manager depend on the browser settings. In Internet Explorer, select the **Tools > Internet Options > Advanced > Multimedia > Play animation in webpages** option to ensure animations display properly.

To launch TRITON Manager, do one of the following:

- On Windows machines, go to **Start > Programs > Websense**, and then select **TRITON Manager**.
- Double-click the TRITON Manager shortcut placed on the desktop during installation.

- Open a supported browser on any machine in your network and enter the following:

  ```
  https://<IP_address_or_hostname>:9443/triton/
  ```

  Substitute the IP address or hostname of the TRITON machine. It is recommended that you use the IP address, especially when launching TRITON Manager from a remote machine.

After installation, the default user, **admin**, has full administrative access to all TRITON modules. The account cannot be deleted, and the user name cannot be changed. The admin password is configured during installation.

At the logon page, enter your **User name** and **Password**, then click **Log On**. If your organization is using two-factor authentication, see *Logging on with certificate authentication*, page 4.

Note

If you are using a local user name created in TRITON Manager and that user name and password match a network account user name and password, the local account takes precedence.

If you are unable to connect to TRITON Manager from a remote machine, make sure that your firewall allows communication on that port.

Windows 7 considerations

If you are using the Windows 7 operating system, you may need to run the browser as administrator for it to allow ActiveX controls.

1. Right-click the browser application and select **Run as administrator**.
2. Log on to TRITON Manager and accept the security certificate as described above.

Adobe Flash Player

Adobe Flash Player v8 or beyond is required for the TRITON AP-DATA, TRITON AP-WEB, and TRITON AP-EMAIL dashboards. All the other functions of TRITON Manager can operate without Flash. If you do not already have Flash Player, you are prompted to install it when you log on. Click the link that is supplied and download Flash Player from the Adobe download center.

Logging on with RSA® SecurID authentication

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

If you are using RSA SecurID authentication, when you access the TRITON Manager URL:

- TRITON Manager detects that RSA SecurID authentication is enabled and available, and displays the RSA version of the logon screen. Note that the "Forgot my password" link on this screen does not apply to SecurID passcodes.
- You provide your two-factor authentication credentials as defined by your organization. For example, your SecurID user name might be your email address or network logon name. The passcode is usually your PIN combined with a token code supplied by a separate hardware or software token: the format depends on the configuration defined by your organization.
- The authentication mechanism searches the local repository for a user profile that matches the user name you typed. If there is no match, the search is repeated in the directory service. If a network user is found then TRITON Manager looks for groups that have been assigned permissions in the system, and if an intersection is found between the groups then the RSA logon proceeds.
- Next, the TRITON Manager custom agent checks the SecurID user name, and the passcode, against the Authentication Manager. If authentication fails, the authentication request falls back to TRITON administrator credentials if configured; otherwise you cannot log on.

If you have enabled RSA SecurID authentication, and you encounter an issue where authentication is failing, you can still log on to TRITON Manager as follows:

1. Open a browser on the TRITON Management Server machine. You can access the machine using a Remote Desktop Connection.
2. Go to the URL https://127.0.0.1:9443/triton (or https://localhost:9443/triton).
3. Log on using the **admin** user name and password.

You can then configure your RSA SecurID authentication options to provide a fallback for your other administrators. See *Configuring two-factor authentication*, page 27.

Logging on with certificate authentication

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

If you are using certificate authentication, you do not usually see the logon page. Instead, when you access the TRITON Manager URL:

1. The manager detects whether a client certificate is installed.
2. You provide your two-factor authentication credentials as defined by your organization.
3. After successful authentication, TRITON Manager receives the client certificate and checks that it matches the signature in the uploaded root CA certificates.
4. If the signature matches, TRITON Manager checks for a full match with the certificates that you have either uploaded to the manager, or imported from your user directory.
5. If a match is found, you are logged on to the manager.

If no certificate match is found, the logon process depends on the fallback options that have been set up:

- Attribute matching checks if the client certificate contains a property matching a specific LDAP attribute in your user directory.
- Password authentication can be enabled in case certificate matching and attribute matching fails.

If neither of these options is available, you cannot log on without a matching certificate.

If all of your administrator accounts are configured to use certificate authentication, and you encounter an issue where your administrators do not have client certificates or certificate matching is failing, you can still log on to TRITON Manager as follows:

1. Open a browser on the TRITON Management Server machine. You can access the machine using a Remote Desktop Connection.
2. Go to the URL https://127.0.0.1:9443/triton (or https://localhost:9443/triton).
3. Log on using the **admin** user name and password.

You can then configure your certificate authentication options to provide a fallback for your other administrators. See *Configuring two-factor authentication*, page 27.

Security certificate alerts

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

An SSL connection is used for secure, browser-based communication with TRITON Manager. This connection uses a security certificate issued by Forcepoint LLC. Because the supported browsers do not recognize Forcepoint LLC, as a known Certificate Authority, a certificate error is displayed the first time you launch TRITON Manager from a new browser. To avoid seeing this error, you can install or permanently accept the certificate within the browser.

Once the security certificate has been accepted, the TRITON Manager logon page is displayed in the browser window.

Note

If you are using Internet Explorer, the certificate error will still be present after you accept the certificate. You must close and reopen your browser to remove the error message.

TRITON Manager session time outs

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

A TRITON Manager session ends 30 minutes after the last action taken in the user interface (clicking from page to page, entering information, caching changes, or saving changes). A warning message is displayed 5 minutes before session end.

- If there are uncached or unsaved changes, the changes are lost when the session ends. Remember to save and deploy changes regularly.

- If TRITON Manager is open in multiple tabs of the same browser window, all instances share the same session. If the session times out in one tab, it times out in all tabs.
- If TRITON Manager is open in multiple browser windows on the same computer, the instances, by default, share the same session.

  If the session times out in one window, it times out in all windows.
- In the following instances, you can open multiple TRITON instances that do not share a session. In these situations, if one window times out, the others are not affected.
  - Use the File > New Session command to open a new Internet Explorer 8 or 9 window.
  - Use Internet Explorer to open one connection to TRITON Manager, and then use Firefox or Chrome to open another connection.

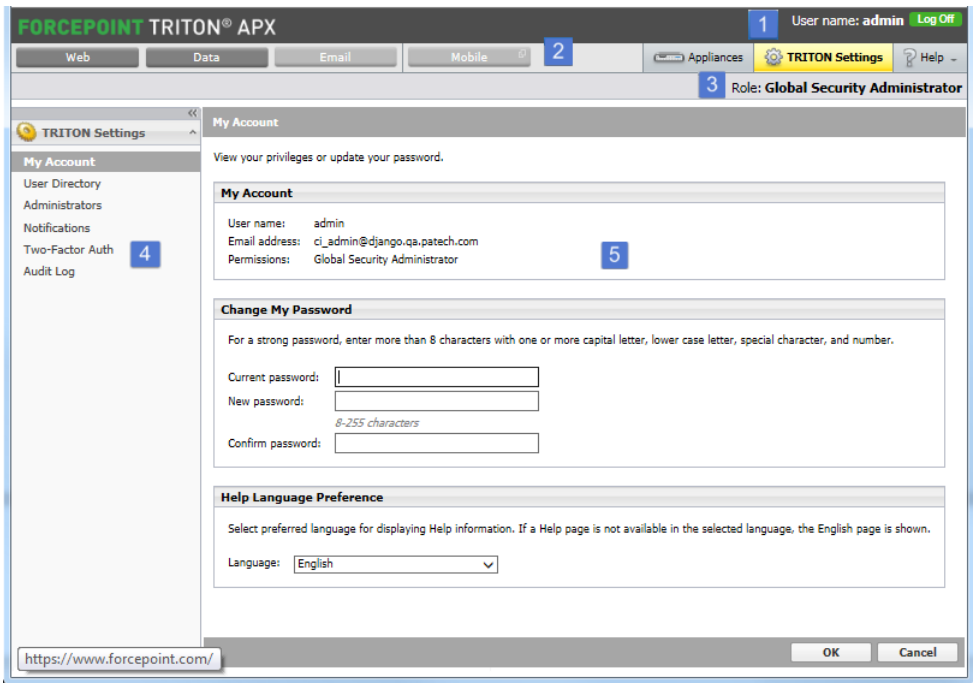
If you close the browser without logging off from TRITON Manager, or if the remote machine from which you are accessing a TRITON module shuts down unexpectedly, you may be temporarily locked out. The software typically detects this issue within about 2 minutes and ends the interrupted session, allowing you to log on again.

Note that if you have a second browser already running in this scenario, you may not be able to log on again for a longer period. If this occurs, close all browsers: The software then can correctly detect the dropped TRITON logon session and you should be able to log on with a new browser session within 2 minutes.

Navigating in TRITON Manager

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

The TRITON Settings interface can be divided into 5 main areas:



1. Banner
2. TRITON toolbar
3. Module toolbar
4. Navigation pane
5. Content pane

The **banner** shows:

- Your current **logon account**
- A **Log Off** button, for when you're ready to end your administrative session

The **TRITON toolbar** indicates which module is active, and lets you launch other TRITON modules. It also provides access to **Help**, tutorials, the Technical Library, and other useful information.

When you log on to TRITON Manager, the module you last accessed is active and the button for that module in the TRITON toolbar is yellow. Buttons for modules that are installed but not currently active are blue, and buttons for uninstalled modules are grey.

The **module toolbar** contains information and options relevant to the module that is currently active. If you are configuring TRITON settings or appliances, it contains your TRITON administrator permissions.

The **navigation pane** contains the available navigation choices for the TRITON module or TRITON configuration option that is currently selected. The **content pane** varies according to the selection in the navigation pane.

For more information about specific modules, see:

- TRITON AP-DATA Help
- TRITON AP-EMAIL Help
- TRITON AP-WEB Help

Managing your account through the My Account Portal

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Forcepoint LLC, maintains a customer portal at My Account that you can use to access product updates, patches and hotfixes, product news, evaluations, and technical support resources for your software.

When you create an account, the account is associated with your Forcepoint subscription key or keys. This helps to ensure your access to information, alerts, and patches relevant to your product and version.

Multiple members of your organization can create My Account logons associated with the same subscription key.

Forcepoint technical support

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Technical information about your software and services is available 24 hours a day at support.forcepoint.com, including:

- the searchable Forcepoint Knowledge Base (made up of a Solution Center, Technical Library, and customer forums)
- Webinars and show-me videos
- product documents and in-depth technical papers
- answers to frequently asked questions

For additional questions, click the **Contact Support** tab at the top of the page.

The contact page includes information for finding solutions, opening an online support case, and calling Forcepoint Technical Support.

For faster phone response, please use your **Support Account ID**, which you can find in the Profile section at My Account.

For telephone requests, please have ready:

- Forcepoint subscription key
- Access to the management console for your solutions (for example, TRITON Manager, Appliance manager, Content Gateway manager)
- Access to the machine running reporting tools and the database server (Microsoft SQL Server or SQL Server Express)
- Familiarity with your network's architecture, or access to a specialist

2 Configuring TRITON Settings

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

TRITON Manager helps you manage Web, data, and email module configuration, policies, and reporting from a central management console.

To facilitate this centralized management, Global Security Administrators (including the default **admin** account) can use **TRITON Settings** to create and configure administrator accounts with:

- Full management access to all TRITON modules
- Full management access to a single TRITON module
- Limited access (for example, reporting-only access) to one or more TRITON modules

See *Introducing administrators*, page 15.

Note

When you make changes to TRITON settings, it can take between 30 and 90 seconds for the changes to propagate to other TRITON modules. For example, if you create an administrator for TRITON AP-DATA, it may take a minute or two for that administrator to appear in the Data Security manager.

TRITON Settings can also be used to:

- View account information and change passwords. See *Viewing your account information*, page 12.
- Set up a connection to a directory service to allow administrators to use their network accounts to log on to TRITON Manager. See *Setting user directory information*, page 12.
- Configure a connection to an SMTP server so that administrators can receive email notifications when they are granted access to TRITON Manager or when their account changes. This also allows administrators to request a password reset, when needed. See *Setting email notifications*, page 25.
- Configure two-factor authentication for administrators. See *Configuring two-factor authentication*, page 27.

- Audit administrator logon attempts and changes to TRITON Settings. See *Audit log*, page 33.

Viewing your account information

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Use the **TRITON Settings > My Account** page to view permissions information for your account, and to select a preferred language for viewing Help information.

If you have been assigned a local user name and password for TRITON Manager, you can also change your password on this page.

If you log on to TRITON Manager with network credentials, password changes are handled through your network directory service. Contact your system administrator for assistance.

The permissions allocated to your account are shown in the toolbar above the page:

- Global Security Administrator means you have full access to all TRITON Manager settings and all policy, reporting, and configuration settings in all of the modules that are part of your subscription. See *Global Security Administrator*, page 15.
- If you do not have Global Security Administrator permissions, the TRITON modules you can access and manage are listed.

To change your password:

1. Enter your **Current password**.
2. Enter and confirm a **New password**.
   - The password must be at least 8 characters.
   - The password must include at least one uppercase letter, lowercase letter, number, and special character (such as hyphen, underscore, or blank).
3. Click **OK** to save your changes.

To select a language other than English as your preferred Help language, select an entry in the **Language** drop-down list. Note that not all Help pages are available in all languages. If a particular Help page is not available in the selected language, the English page is displayed.

Setting user directory information

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Use the **TRITON Settings > User Directory** page to configure directory communication for administrators using their network accounts. The same directory must be used to authenticate all administrative users.

- A user directory stores information about a network's users and resources.
- To allow administrators to use their network accounts to log on to TRITON Manager, you must configure the manager to retrieve information from your user directory.

Note

User directory configuration for administrators is performed separately from directory service configuration for end users. Set up end user directory service configuration within each TRITON module.

TRITON Manager can communicate with the following LDAP (Lightweight Directory Access Protocol) directories:

- Windows Active Directory (Native Mode)
- Novell eDirectory
- Oracle Directory Service
- Lotus Notes/Domino

It can also communicate with other generic LDAP-based directories.

Note that:

- Duplicate user names are not supported in an LDAP-based directory service. Ensure that the same user name does not appear in multiple domains.
- If you are using Windows Active Directory or Oracle Directory Service, user names with blank passwords are not supported. Make sure that all users have passwords assigned.

To enable administrators to log on to TRITON Manager using a network account:

1. Select your user directory from the **User directory server** list.
2. Enter the **IP address or host name** to identify the directory server.
3. Enter the **Port** that the software should use to communicate with the directory.
4. Specify the **User distinguished name** and **Password** for the administrative account the software should use to retrieve user name and path information from the directory.
   - The account must be able to query and read from the directory, but does not need to be able to make changes to the directory, or be a domain administrator.
   - Enter the account details as a single string in the **User distinguished name** field. You can use the format "CN=user, DC=domain" or, if your organization uses Active Directory, "domain\username".
5. Click **Test Connection** to confirm that the directory exists at the specified IP address or name and port number, and that the specified account can connect to it.

6. Enter the **Root naming context** that TRITON Manager should use to search for user information. This is required for generic LDAP directories, Lotus Notes/ Domino, and Oracle Directory Service, and optional for Active Directory and Novell eDirectory. If you supply a value, it must be a valid context in your domain.

   If the Root naming context field is left blank, the software begins searching at the top level of the directory service.

   Note

   Avoid having the same user name in multiple domains. If the software finds duplicate account names for a user, the user cannot be identified transparently.

7. If your LDAP schema includes nested groups, mark **Perform additional nested group search**.
8. To encrypt communication with the directory service, mark **Use SSL encryption**.
9. If your directory service uses LDAP referrals, indicate whether the software should follow the referrals.
10. If you have selected Generic Directory, also configure the following settings:
    - **Email attribute**: The attribute name used to locate a user's email address in LDAP entries. The default is **mail**.
    - **User logon ID attribute**: The attribute name used to locate a user's logon ID in LDAP entries.
    - **User logon filter**: The filter to apply when searching for user details at logon. This string must contain the **%uid** token, which is then replaced with the user name entered by the user when logging on.
    - **User lookup filter**: The filter used to find users for import on the Add Network Account page. You can enter **%query** in this field as a placeholder, and then click **Refine search** on the Add Network Account page to enter a new context for finding network users.
    - **Group object class** (optional): The LDAP object class that represents a group. The default is **group**.
    - **Group Properties**: Specify whether your directory schema uses the memberOf attribute. If it does, in the **Group attribute** field enter the attribute used to reference the groups that the user is a member of.

      If it does not, in the **User group filter** field enter the query used to resolve groups containing the specific user. You can enter **%dn**, which will be replaced by the DN of the user.

11. Click **OK**.

Note

If you change your user directory settings at a later date, existing administrators become invalid unless you are pointing to an exact mirror of the user directory server. If the new server is not a mirror, you may not be able to distinguish between your new and existing users.

Introducing administrators

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Administrators can access TRITON Manager to configure one or more security solutions, manage policies, generate reports, or perform some combination of these tasks. The specific permissions available depend on the type of administrator.

- Global Security Administrators have full access and management permissions in all available TRITON modules. See *Global Security Administrator*, page 15.
- Other types of administrators have more restricted access to TRITON modules. An administrator may be given permission to manage or audit one or more TRITON modules using the same account. See *TRITON administrators*, page 16.

You can identify administrators using their network logon credentials, or you can create accounts used only to access TRITON Manager. See *Adding a network account*, page 20, and *Adding a local account*, page 18.

Global Security Administrator

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

A default Global Security Administrator role is created during installation, and the default user, **admin**, is assigned to this role. When you first log on with the password set during installation, you have full administrative access to all configuration settings in TRITON Manager, and also the following permissions in the modules that are part of your subscription:

- **Web module:** Added to the Super Administrator role with unconditional permissions.
- **Data module:** Assigned Super Administrator permissions.
- **Email module:** Assigned Super Administrator permissions.

You also have full permissions to manage and transparently log on to all appliances registered with this instance of TRITON Manager.

The permissions given to a Global Security Administrator within the individual TRITON modules cannot be modified.

The admin account does not appear in the list of administrators for the Super Administrator role. It cannot be deleted, and its permissions cannot be modified.

You can add further Global Security Administrators as needed. Creating multiple Global Security Administrators ensures that if the primary Global Security Administrator is not available, another administrator has access to all TRITON policy and configuration settings.

TRITON administrators

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

TRITON administrators are given access to one or more TRITON modules (Web, Data, Email). They can also be granted access to the Mobile portal, one or more appliances registered with TRITON Manager, and one or more Content Gateway Manager instances.

Administrators can be given **access** to one or more modules, or **access and account management** permissions. The permissions these administrators have in each module depend on how administrators are configured within the module. By default the following permissions are allocated:

- Web module
  - **Access**: the administrator is not added to any roles, and can only access the Status > Dashboard and Status > Alerts pages.
  - **Access and account management**: the administrator is added to the Super Administrator role with unconditional permissions.

  Administrator permissions can be changed in the Web module on the **Policy Management > Delegated Administration** page.
- Data module
  - **All options**: the administrator is assigned the Default access role, with access to the Incidents & Reports, Today, and My Settings pages.

  Administrator permissions can be changed in the Data module on the **Settings > General > Authorization > Administrators**, and **Settings > General > Authorization > Roles** pages.
- Email module
  - **Access**: the administrator is assigned the default Reporting permissions.
  - **Access and account management**: the administrator is assigned Super Administrator permissions by default.

  Administrator permissions can be changed in the Email module on the **Settings > General > Administrator Accounts** page.

For appliances, administrators can be given **full access** or **limited access** to the appliances registered in TRITON Manager.

- Full access enables the administrator to register and unregister appliances, and to access appliances directly from TRITON Manager. Access is via single sign-on if configured (see *Configuring an existing appliance for single sign-on*, page 38).

- Limited access enables the administrator to access appliances, but not register or unregister them. Access can be to all appliances, including those added subsequently, or to specifically selected appliances.

Administrators with account management permissions can also edit and delete other administrators in TRITON Manager, subject to the limitations of the permissions they have been allocated.

Administrators who log on to TRITON Manager with a local user account can also change their own TRITON password (see *Viewing your account information*, page 12).

Once shared administrator accounts have been configured, an administrator logged on to one TRITON module (for example, Web) can use the TRITON toolbar to switch to a different module (Data or Email) without needing to log on a second time.

Enabling access to TRITON Manager

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Use the **TRITON Settings > Administrators** page to create and manage the accounts that administrators use to access TRITON Manager.

Note

This page is available only to Global Security Administrators and administrators that have permission to manage at least one TRITON module.

In deployments that include a combination of web, email, and data solutions, administrator accounts can be given individual or joint access to the available TRITON modules.

Next to the User Name column, the Type column displays the type of each administrator account:

- **Local accounts** are created specifically for use within TRITON Manager.
- **Network accounts** are accounts from a supported directory service that have been granted access to TRITON Manager (see *Setting email notifications*, page 25).

To add an account, click either **Add Local Account** or **Add Network Account** (see *Adding a local account*, page 18, and *Adding a network account*, page 20).

Note

If you have enabled RSA SecurID authentication on the **TRITON Settings > Two-Factor Authentication** page, any administrator accounts you add on this page are used only as a fallback if the RSA Authentication Manager cannot be reached. You must mark the **Fall back to other authentication options** box on the Two-Factor Authentication page for the administrator accounts to be available. See *Configuring two-factor authentication*, page 27.

If an administrator account has an exclamation mark icon next to the name on this page, the account does not have an email address associated with it. This means the administrator will not receive notifications of password changes or permission updates. Edit the administrator details to add an email address.

If you are viewing this page as a TRITON administrator with permission to manage at least one TRITON module, you can manage and delete only administrator accounts for those modules.

Global Security Administrators can manage and delete any existing accounts. To delete an account, mark the check box next to the account name and click **Delete**.

Important

If you delete an administrator account, actions performed by this administrator will no longer appear in the TRITON AP-DATA incident history. To preserve administrator actions, it is recommended that you do not delete the account, but instead limit the administrator's role in the Data module.

Adding a local account

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Related topics:

- *Enabling access to TRITON Manager*, page 17
- *Adding a network account*, page 20
- *Editing a local account*, page 22

Use the **TRITON Settings > Administrators > Add Local Account** page to add local user accounts.

1. Enter a unique **User name**, up to 50 characters.
   - The name must be between 1 and 50 characters long, and cannot include any of the following characters:

     `* < > ' ‘ { } ~ ! $ % & @ # . " | \ & + = ? / ; : , ^ ( )`
   - User names can include spaces and dashes.
2. Enter a valid **Email address** for the user.

   This email address is used to send account information to the new administrator.
3. Enter and confirm a **Password** (8-255 characters) for this user.

   The password must include at least one each of the following:
   - uppercase letter
   - lowercase letter
   - number
   - special character (such as hyphen, underscore, or blank)

   Note

   If certificate authentication is enabled and password authentication is disabled on the **TRITON Settings > Two-Factor Authentication** page, password logon is not available for the local account.
4. To create an administrator with full permissions across TRITON Manager and all of the modules and appliances in your subscription, select **Global Security Administrator**.

   Note

   Only Global Security Administrators can create other Global Security Administrators.
5. To send account information and access instructions to the new administrator via email, mark **Notify administrator of the new account via email**.

   To send administrator emails, you must set up SMTP details on the Notifications page. You can also customize the contents of the email message on the Notifications page (see *Setting email notifications*, page 25).
6. To require the administrator to change the account password the first time he or she logs on to TRITON Manager, mark **Force administrator to create a new password at logon**.
7. If certificate authentication is enabled on the **TRITON Settings > Two-Factor Authentication** page:
   a. Click **Certificate Authentication**.
   b. Browse to the location of the certificate to use for administrator authentication for this account.
   c. Click **Upload Certificate**.

For more information, see *Configuring two-factor authentication*, page 27.

8. If this account is not a Global Security Administrator, under **Module Access Permissions**, select the permissions you want to give to the new administrator.
   - Choose a setting under each of the available options (**Web**, **Data**, **Email**) to give the new administrator permissions to manage one or more of the TRITON modules. The options available depend on the modules in your subscription.

     For each module, choose whether the new administrator has:
     - no access to that module
     - only access to the module
     - both access and the ability to manage other administrators in that module.

     For more information see *TRITON administrators*, page 16.

     Note
     You can assign access permissions only for the TRITON modules where you have management permissions.

   - If your deployment includes one or more appliances, you can grant the administrator:
     - no appliance access
     - full access to all appliances
     - limited access to appliances

     If you select limited access, indicate whether the administrator can access all appliances or only specified appliances.
9. When you are finished making changes, click **OK**.

Adding a network account

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Related topics:

- *Setting email notifications*, page 25
- *Adding a local account*, page 18
- *Editing a network account*, page 24

Use the **TRITON Settings > Administrators > Add Network Account** page to add users defined in a supported directory service as TRITON administrators.

Enter keywords to search on in the **Search** field to find the accounts that you want to add as TRITON administrators. Optionally, you can use the asterisk wildcard (*) as part of your search.

By default, the search context for your search is the default domain context from the Directory Service page (see *Setting email notifications*, page 25). You can edit this

context by clicking **Refine search** and entering a new search context in the field that appears. You can revert to the default context by clicking **Restore default**.

If you are using Active Directory, for users the Email, Login Name, and Display Name fields in your selected context are searched. If you are using Novell eDirectory, Oracle Directory Service, or Lotus Notes/Domino, for users the Email, Display Name, Username, and Common Name (CN) fields are searched. For all directory services, the CN field is searched for groups.

The search results list both users and groups that match the specified keywords, and display both user name and email address for the network account. To add a user or group as an administrator, mark the check box next to the account name, and then click the right arrow (>) to add the account to the Selected accounts list.

To delete a user from the Selected accounts list, mark the check box next to the account name, and then click the left arrow (<).

If certificate authentication is enabled on the **TRITON Settings > Two-Factor Authentication** page (see *Configuring two-factor authentication*, page 27), click **Certificate Authentication** to upload or import the certificate used to authenticate the selected administrators during TRITON Manager logon.

- Click **Import from LDAP** to import the certificate from your user directory.
- Click **Upload Certificate** to browse to the location of the certificate and upload it.

When the certificate has been imported or uploaded successfully, the certificate name, expiration date, issuer, and source information are displayed in the Certificate Authentication area of the page.

Once you have added one or more accounts to the Selected accounts list, indicate whether to **Notify administrator of the new account via email**. To send administrator emails, you must set up SMTP details on the Notifications page. You can also customize the contents of the email message on the Notifications page (see *Setting email notifications*, page 25).

Next, select the access permissions you want to give to the new administrators.

- Select **Global Security Administrator** to create an administrator with full permissions across TRITON Manager and all of the modules and appliances in your subscription.

  Note
  Only Global Security Administrators can create other Global Security Administrators.

- If the accounts are not Global Security Administrators, under **Module Access Permissions**, select the permissions you want to give to the new administrators.
  - Choose a setting under each of the available options (**Web**, **Data**, **Email**) to give the new administrator permissions to manage one or more of the TRITON modules. The options available depend on the modules in your subscription.

For each module, choose whether the new administrator has:

- no access to that module
- only access to the module
- both access and the ability to manage other administrators in that module.

For more information see *TRITON administrators*, page 16.

Note

You can assign access permissions only for the TRITON modules where you have management permissions.

- If you have one or more appliances as part of your subscription, choose whether the new administrator has:
- If your deployment includes one or more appliances, you can grant the administrator:
  - no appliance access
  - full access to all appliances
  - limited access to appliances

  If you select limited access, indicate whether the administrator can access all appliances or only specified appliances.

When you are done selecting administrator accounts, click **OK.**

Editing a local account

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Use the **TRITON Settings > Administrators > Edit Local Account** page to edit existing local user accounts.

1. To change the **User name**, enter a unique name up to 50 characters.
   - The name must be between 1 and 50 characters long, and cannot include any of the following characters:

     `* < > ' { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,`
   - User names can include spaces and dashes.
2. To change the administrator **Email address**, enter a valid address for the user.

   This email address is used to send account information to the administrator.
3. To reset the administrator's **Password**, enter and confirm a password (8-255 characters).

   The password must include at least one each of the following:
   - uppercase letter
   - lowercase letter
   - number

- special character (such as hyphen, underscore, or blank)

> **Note**
> If certificate authentication is enabled and password authentication is disabled on the **TRITON Settings > Two-Factor Authentication** page, password logon is not available for the local account.

4. To give the administrator full permissions across TRITON Manager and all of the modules and appliances in your subscription, select **Global Security Administrator**.

> **Note**
> Only Global Security Administrators can create other Global Security Administrators.

5. To send account update information to the administrator via email, mark **Notify administrator of the account changes via email**.

> **Note**
> Selecting this option notifies the administrator only of the current changes being made. If you return to make further edits to this or another administrator's details, you will need to mark the option again.

6. To require the administrator to change the account password the next time he or she logs on to TRITON Manager, mark **Force administrator to create a new password at logon**.
7. If certificate authentication is enabled on the **TRITON Settings > Two-Factor Authentication** page:
   a. Click **Certificate Authentication**.
   b. Browse to the location of the certificate that the administrator will authenticate against when logging on to TRITON Manager.
   c. Click **Upload Certificate**.

   For more information, see *Configuring two-factor authentication*, page 27.
8. If this is not a Global Security Administrator account, use the **Module Access Permissions** options to update permissions for the administrator.
   - Choose a setting under each of the available options (**Web**, **Data**, **Email**) to give the administrator permissions to manage one or more of the TRITON modules. The options available depend on the modules in your subscription.

     For each module, choose whether the administrator has:
     - no access to that module
     - only access to the module

- both access and the ability to manage other administrators in that module.

For more information see *TRITON administrators*, page 16.

> **Note**
> You can assign access permissions only for the TRITON modules where you have management permissions.

- If your deployment includes one or more appliances, you can grant the administrator:
  - no appliance access
  - full access to all appliances
  - limited access to appliances

  If you select limited access, indicate whether the administrator can access all appliances or only specified appliances.

9. When you are finished making changes, click **OK**.

Editing a network account

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Use the **TRITON Settings > Administrators > Edit Network Account** page to edit the access and authentication permissions for existing network accounts.

If certificate authentication is enabled on the **TRITON Settings > Two-Factor Authentication** page (see *Configuring two-factor authentication*, page 27), click **Certificate Authentication** to upload or import the certificate that the administrators will authenticate against when logging on to TRITON Manager.

- Click **Import from LDAP** to import the certificate from your user directory.
- Click **Upload Certificate** to browse to the location of the certificate and upload it.

When the certificate has been imported or uploaded successfully, the certificate name, expiration date, issuer, and source information are displayed in the Certificate Authentication area of the page. Click **Import New from LDAP** to import a new certificate from your user directory, replacing the existing certificate.

Click **Remove Certificate** to delete the certificate from this network account. If you remove the certificate, this network account cannot use two-factor authentication.

To change the access permissions for the network account:

- Select **Global Security Administrator** to give the administrator full permissions across TRITON Manager and all of the modules and appliances in your subscription.

> **Note**
> Only Global Security Administrators can create other Global Security Administrators.

- If this is not a Global Security Administrator account, use the **Module Access Permissions** options to update permissions for the administrator.
  - Choose a setting under each of the available options (**Web**, **Data**, **Email**) to give the administrator permissions to manage one or more of the TRITON modules. The options available depend on the modules in your subscription.

    For each module, choose whether the administrator has:

    - no access to that module
    - only access to the module
    - both access and the ability to manage other administrators in that module.

    For more information see *TRITON administrators*, page 16.

    Note
    You can assign access permissions only for the TRITON modules where you have management permissions.

  - If your deployment includes one or more appliances, you can grant the administrator:
    - no appliance access
    - full access to all appliances
    - limited access to appliances

    If you select limited access, indicate whether the administrator can access all appliances or only specified appliances.

When you are done editing administrator permissions, click **OK.**

Setting email notifications

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Use the **TRITON Settings > Notifications** page to set up the SMTP server used for all email notifications from TRITON Manager and to configure the notification email messages sent to administrators.

Note
This page can be viewed and edited only by Global Security Administrators.

First, establish a connection with your SMTP server so that email notifications can be sent:

1. Enter the **IP address or host name** and **Port** of the SMTP server machine.
2. Enter the **Sender email address** to use in notifications.
3. Enter a **Sender name** to appear with the From email address. This is useful to make it clear to administrators that the email is related to TRITON Manager.

Next, review the templates used for administrator notifications. There are 3 available templates:

- **New Account**: Notifies an administrator of their new TRITON account. Typically, this template includes the new logon name and password, and a summary of the permissions allocated to the administrator.
- **Edit Account**: Notifies an administrator of any changes to their TRITON account. Typically, this includes any information that might be changed and would need to be communicated to the administrator, such as their logon name, password, and permissions.
- **Forgot Your Password**: Confirms to an administrator who has clicked the "Forgot Your Password" link on the TRITON logon page that their password has been reset. Typically, this includes the temporary password and expiration details for that password.

Each template contains default text that you can use or modify, and includes some available variables. At the time the email is sent to the administrator, these variables are replaced either with user-specific data or with values configured elsewhere in the system. Variables are always surrounded by percentage symbols, such as %Username%.

To modify a notification message:

1. Select one of the Email Notification Templates tabs: New Account, Edit Account, or Forgot Your Password.
2. Enter a suitable subject header for the email message. For example, for a new account, you might use "Welcome to TRITON" or "Your new TRITON Manager account."
3. Modify the message body as required. To add a variable, click **Insert Variable** and select from the drop-down list:

Variable	Description
%TRITON URL%	The URL used to access TRITON Manager.
%Username%	The administrator's TRITON username.
%Password%	The administrator's TRITON password. This may be the temporary password assigned to an administrator who used the "Forgot Your Password" link. This password is valid for 30 minutes; an administrator logging on during that time is prompted to enter a new password.
%Permissions%	The permissions allocated to the administrator.

Note

If you are using all or part of the default notification text, you can only include variables at the end of the default message.

4. To return to the default notification text at any time, click **Restore Default**, then click **OK** to confirm.

Configuring two-factor authentication

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Use the **TRITON Settings > Two-Factor Auth** page to manage the use of two-factor authentication for administrator logons.

Note
Only Global Security Administrators can access this page.

Two-factor authentication requires administrators to provide 2 forms of identification when logging on to TRITON Manager.

TRITON administrators can be granted single sign-on access to other TRITON management consoles (Appliance Manager and Content Gateway Manager). To use this functionality with two-factor authentication:

- **Appliance Manager**: Set up single sign-on permissions for administrator accounts (see *Configuring an existing appliance for single sign-on*, page 38).
- **Content Gateway Manager**: Disable password authentication for Content Gateway Manager (see "Configuring Content Gateway for two-factor authentication" in the Content Gateway Help).

Access to TRITON Mobile Security is not covered by two-factor authentication: you must log on to the cloud-based console using your regular username and password.

The following methods are available:

- RSA SecurID® authentication (see *How does RSA SecurID authentication work?*, page 29)
- Certificate authentication (see *How does certificate authentication work?*, page 31).

If you choose to enable RSA SecurID authentication:

- You must be running RSA Authentication Manager 6.1.2 or higher.
- Ensure only one NIC is configured and enabled on your TRITON Management Server.
- You must first create a custom agent for TRITON Manager in your RSA Authentication Manager (see *Creating a custom agent for RSA SecurID authentication*, page 29).
- Certificate authentication is automatically disabled. If you have previously enabled certificate authentication and then enable RSA SecurID authentication, a warning message appears.

To set up TRITON Manager RSA SecurID authentication:

1. Mark **Authenticate administrators using RSA SecurID authentication**.
2. Enter a valid **Username** and **Passcode** for RSA SecurID logon.

   The user must be able to authenticate with RSA Authentication Manager, but does not have to be a TRITON administrator.
3. Click **Test Connection to RSA Manager**.

You must successfully test the connection to your RSA Authentication Manager before you can save your changes on this page. The results of the test are displayed next to the Test Connection button; for more information on these results, see *Test Connection to RSA Manager results*, page 30.

1. To allow administrators to log on to TRITON Manager if RSA authentication is unavailable, mark **Fall back to other authentication mechanisms...**.

   Selecting this option means that any administrators configured on the **TRITON Settings > Administrators** page can log on using their local or network credentials as a fallback. If you do not select this option, RSA authentication is the only option for all administrators except the **admin** account created during installation.
2. Click **OK**.

To set up TRITON Manager certificate authentication:

1. Mark **Authenticate administrators using client certificate authentication**.
2. To enable attribute matching, under Certificate Matching mark **Use attribute matching as a fallback method** and select whether it applies to all administrators, or only administrators without certificates in TRITON Manager.

   To configure the attributes used for matching, click **Configure Attribute Matching**, then see *Setting up attribute matching*, page 32.
3. To import certificates from your user directory for network administrators, click **Import Administrator Certificates**.

   When certificates are successfully imported, a success message is displayed at the top of the page. If any of the certificates are not imported correctly, you can upload a certificate for each network administrator on the **TRITON Settings > Administrators > Edit Network Account** page.
4. Click **Add** under **Root Certificates** to add a root certificate for signature verification. There must be at least one root certificate in TRITON Manager for two-factor authentication to operate.
5. Browse to the location of the root certificate file, then click **Upload Certificate**.
6. Whenever you add or change a root certificate, you must create a new master certificate file and copy that file to the Websense TRITON Web Server service. Click **Create Master Certificate File** to create the new file, then see *Deploying the master certificate file*, page 32 for further information.

7. To enable password authentication as a fallback method, mark **Allow password authentication to log on to TRITON Manager** and select whether it applies to all administrators, or only administrators without certificates in TRITON Manager.

   Note
   The **admin** account created during installation can always log on from the TRITON Management Server machine using password-based authentication.

8. Click **OK**.

How does RSA SecurID authentication work?

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

When you enable RSA SecurID authentication on the Two-Factor Authentication page, the logon process for an administrator accessing the TRITON Manager URL is as follows:

- TRITON Manager detects that RSA SecurID authentication is enabled and available, and displays the RSA version of the logon screen. Note that the "Forgot my password" link on this screen does not apply to SecurID passcodes.
- The administrator provides their two-factor authentication credentials as defined by your organization. For example, their SecurID user name might be their email address or network logon name. The passcode is usually their PIN combined with a token code supplied by a separate hardware or software token: the format depends on the configuration chosen by your organization.
- The authentication mechanism searches the local repository for a user profile that matches the user name typed by the user. If there is no match, the search is repeated in the directory service. If a network user is found then TRITON Manager looks for groups that have been assigned permissions in the system, and if an intersection is found between the groups then the RSA logon proceeds.
- Next, the TRITON Manager custom agent checks the SecurID user name, and the passcode typed by the user, against the Authentication Manager. If authentication fails, the authentication request falls back to TRITON administrator credentials if configured; otherwise the administrator cannot log on.

The custom agent supports the creation of a new PIN, if required, as part of the authentication process. This might be entered by the administrator or generated by the system. If applicable the security criteria for the PIN are displayed on screen.

Creating a custom agent for RSA SecurID authentication

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

To enable and use RSA SecurID two-factor authentication, you must first use RSA Authentication Manager to create a custom agent for TRITON Manager. This agent is

used to communicate with the RSA Authentication Manager server when you test the connection on the **TRITON Settings > Two-Factor Authentication** page, and during the logon process.

To create a custom agent:

1. In RSA Authentication Manager, add an Agent Host with the following minimum settings:

Name	Hostname where TRITON Manager is running. This must resolve to a valid IP address on the local network.
Network Address	IP address where TRITON Manager is running.
Agent Type	Select **Standard Agent**.
Encryption Type	Select **DES**.

2. Click **Generate Configuration Files**.
3. Copy the RSA Authentication Manager configuration file (sdconf.rec) to the following directory on the TRITON Management Server: C:\Program Files (x86)\Websense\EIP Infra\tomcat\wbsnData\rsaSecurID\.

> **Note**
> By default, the sdconf.rec file is located in the ACE\Data folder on the RSA Authentication Manager server.

4. If a node secret file (securid) exists, copy this file to the above directory as well.
5. If you are logged on to TRITON Manager, log off.
6. On the TRITON Management Server, go to **Start > Administrative Tools > Services**.
7. Right-click the **Websense TRITON Manager** service and select **Restart**.

Test Connection to RSA Manager results

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

You must test the connection to your RSA Authentication Manager to enable RSA SecurID authentication. If you see a “Connection succeeded” message, TRITON Manager was able to both connect to your RSA Manager and authenticate with the credentials you provided, and you can save your settings on the Two-Factor Authentication page.

The table below provides more information on the other messages you may see.

Message	Description
Connection succeeded. PIN or next token code required for successful logon.	TRITON Manager has successfully connected to your RSA Manager but could not authenticate with the passcode provided. You can still enable RSA SecurID authentication and save your settings; however, note that the Passcode field does not include the credentials required for a successful logon. This might be your PIN, or the next token code on your RSA SecurID software or hardware token, or a combination of the two.
Connection succeeded. Authentication failed: unknown user or incorrect password.	TRITON Manager has successfully connected to your RSA Manager but could not authenticate with the credentials you provided. Check that the username and passcode you entered are valid.
Connection failed: could not find RSA agent configuration file.	Ensure you have followed the steps in *Creating a custom agent for RSA SecurID authentication*, page 29, to create a custom agent in your RSA Manager. The **Authenticate administrators using RSA SecurID authentication** check box stays in a partially-selected state, and you cannot enable RSA SecurID authentication until you have successfully re-tested the connection.
Connection failed. Verify your configuration settings.	TRITON Manager could not connect to your RSA Manager. The **Authenticate administrators using RSA SecurID authentication** check box stays in a partially-selected state, and you cannot enable RSA SecurID authentication until you have successfully re-tested the connection.

How does certificate authentication work?

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

When you enable certificate authentication on the Two-Factor Authentication page, the logon process for an administrator accessing the TRITON Manager URL is as follows:

- TRITON Manager detects whether a client certificate is installed. If more than one certificate is available, the administrator is asked to select the certificate that allows access to the manager.
- The administrator provides their two-factor authentication credentials as defined by your organization. For example, this could be through the use of the Common Access Card (CAC) and a card reader.
- After successful authentication, TRITON Manager receives the client certificate and checks that it matches the signature in the uploaded root CA certificates. If the signature matches, TRITON Manager checks for a full match with the certificates that you have either uploaded to TRITON Manager, or imported from your user directory. If a match is found, the administrator associated with the two-factor authentication credentials is logged on to the manager.

- If no certificate match is found and you have set up attribute matching as a fallback option, a check is performed to see if the client certificate contains a property matching a specific LDAP attribute in your user directory. If a match is found, the administrator associated with the two-factor authentication credentials is logged on to the manager.

If all configured certificate and attribute matching fails, or if the administrator does not have a client certificate, you can allow password authentication as a fallback option. If password authentication is disabled, administrators without matching certificates cannot log on.

Deploying the master certificate file

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

When you create a new master certificate file following changes to your certificate authentication root certificate, you must update the Websense TRITON Web Server service with the new file. To do this:

1. Go to the directory where you installed TRITON Manager (by default **C:\Program Files (X86)\Websense**), and access the **EIP Infra** directory.
2. Run the script file **replace_2fa_certificate.bat**.

The script file copies the new master certificate file that you have created to the Websense TRITON Web Server service, and then restarts the service.

Setting up attribute matching

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Use the **TRITON Settings > Two-Factor Authentication > Configure Attribute Matching** page to define the administrator LDAP property that matches against a property in the certificate provided.

1. Under **Administrator Property**, select the property from your user directory that will be used to match against the administrator's certificate. This can be:
   - The administrator **Email address** (local and network accounts)
   - **LDAP distinguished name** (network accounts only)
   - **User name** (local and network accounts)
   - A **Custom LDAP field** (network accounts only)

Note

If you are using a generic LDAP user directory, you must specify a custom field.

2. If you have defined a custom LDAP field, click **Verify Administrator Property** to confirm that the property exists in your user directory. Select a network administrator account to verify against.

   Note
   Verify Administrator Property is available only if you have configured your user directory in TRITON Manager, and you have set up at least one network administrator account.

   When you save the settings on this page, the custom property is imported for all applicable accounts (network only, or local and network accounts) in TRITON Manager. If you need to change this field at a later date, click **Update Property** to import the new attribute matching value.

3. Under **Certificate Property**, select the property in the administrator's logon certificate to match against the LDAP property that you defined:
   - The email (RFC822) attribute of the subjectAltName field. Select this if you are matching against the administrator email address in your user directory
   - The Subject distinguished name, which defines the entity associated with this certificate
   - The unique serial number for each certificate issued by a particular Certification Authority (CA).
4. Click **OK**.

   The properties that you selected are displayed in the Certificate Matching area on the **TRITON Settings > Two-Factor Authentication** page.

Audit log

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Use the **TRITON Settings > Audit Log** page to view actions performed by administrators in the system.

Note
Only Global Security Administrators can access this page.

By default, the displayed actions are sorted by date and time. If a filter is used, the number of displayed actions is shown at the top of the list.

Column	Description
ID	ID number of the action. You can quickly jump to an Audit Log action by entering the ID number in the **Find ID** field and clicking **Find**.
Date & Time	Date and time the action occurred.
Administrator	Name and user name of the administrator that initiated the action in TRITON Manager.
Role	Role of the administrator.
Action Performed	Details of the action. This column may contain variables that are filled in by the system, for example a logon user name.

3 Accessing Appliances

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Forcepoint LLC, offers security appliances with an operating system optimized for analyzing Web and email traffic and content. If you have purchased an appliance-based solution, TRITON Manager enables you to view details of and easily access multiple appliances.

For more information, see:

Managing appliances

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Use the **Appliances > Manage Appliances** page to review the V-Series and X-Series appliances registered (associated) with this TRITON Manager, register additional appliances, or unregister an appliance.

The following information is displayed for each registered appliance:

- IP address for interface C on the appliance
- Appliance hostname
- Security mode: Web, Email, or Web and Email
- Policy source mode (applies only to appliances that include Web Security): full policy source, user directory and filtering, or filtering only
- Description (can be edited on the System page in Appliance Manager)
- TRITON software version (for example, 8.2.0)
- Hardware platform (for example, V5000 or V10000 G2)

Click the arrow next to the appliance IP address to expand the appliance information and see these details. Use the **Expand All** and **Collapse All** buttons to expand or collapse all appliance information.

If the details for an appliance include a Single Sign-On button, you can access that appliance without providing further logon credentials.

- To register an appliance with TRITON Manager, see *Registering an appliance*, page 36. New appliances can be configured for single sign-on when you add them to TRITON Manager.
- To configure an existing appliance (for example, an appliance upgraded from a previous version) for single sign-on, see *Configuring an existing appliance for single sign-on*, page 38.
- To access an appliance that is not configured for single-sign on, click the appliance's IP address. This opens a logon page in a new browser. Enter your Appliance Manager logon credentials.

Registering an appliance

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

To register a new appliance with TRITON Manager:

1. Click **Register Appliance**.
2. Enter the IP address for network interface C on the appliance.
3. To configure single sign-on from this TRITON Manager to the appliance, mark **Enable single sign-on from TRITON Manager**.
4. Enter the administrator password for the appliance.
5. To specify TRITON administrators who have single sign-on permissions for this appliance, click **User Permissions**.
6. To give an administrator single sign-on permissions, mark the check box next to the user name in the Available users list, and then click the right arrow (>) to add the administrator to the Users with access list.

Note

Global Security Administrators and administrators with full appliance access are greyed out in the Users with access list, because they have single sign-on access by default, and this cannot be changed.

7. Click **Save**.

   If successful, an Appliance Details popup appears confirming the appliance has been added to TRITON Manager, and displaying information retrieved from the appliance.

   An appliance can only be configured for single sign-on from one TRITON Management Server. If another TRITON instance has already registered an appliance with single sign-on, an error message appears. Select **Transfer registration** to transfer the single sign-on to this instance of TRITON Manager, or select **Register without Single Sign-On** to register the appliance and preserve single sign-on configuration on the other TRITON Management Server.

8. To add further appliances, click **Add Another Appliance** and repeat steps 2 to 7 above. If you are finished adding appliances, click **Done**.

If TRITON Manager cannot connect to the IP address that you enter, ensure:

- The IP address you entered is the correct one for the appliance's C interface
- The appliance and appliance manager are both running
- The system clock on the TRITON Manager machine matches the clock on the appliance to within 1 minute

To refresh the information for an appliance, expand the appliance information and click **Refresh Details**. To refresh all of the appliance information on this page, click **Refresh All Appliances**.

To remove an appliance from the list, expand the appliance information and click **Unregister**, then click **Yes** to confirm.

Editing appliance details

To edit an appliance's IP address:

1. Click the arrow next to the current appliance IP address to expand the appliance information.
2. Click the icon to the right of the current IP address.
3. Enter the new IP address for network interface C on the appliance.
4. Click **Save**.

If TRITON Manager cannot connect to the IP address that you enter, ensure:

- The IP address you entered is the correct one for the appliance's C interface
- The appliance and appliance manager are both running
- The system clock on the TRITON Manager machine matches the clock on the appliance to within 1 minute

To change the list of administrators who can access the appliance with single sign-on:

1. Click the arrow next to the current appliance IP address to expand the appliance information.
2. Click the Edit single sign-on user permissions icon in the top right corner of the appliance information pane.
3. To give an administrator single sign-on permissions, mark the check box next to the user name in the Available users list, and then click the right arrow (>) to add the administrator to the Users with access list.

4. To remove single sign-on permissions from an administrator, mark the check box next to the user name in the Users with access list, and then click the left arrow (<) to add the administrator to the Available users list.

   Note
   Global Security Administrators and administrators with full appliance access are greyed out in the Users with access list, because they have single sign-on access by default, and this cannot be changed.

5. Click **Save**.

Configuring an existing appliance for single sign-on

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

1. Click **Configure single sign-on** for the appliance you want to edit.
2. Mark **Enable single sign-on from TRITON Manager**.
3. Enter the administrator password for the appliance.
4. To specify TRITON administrators who have single sign-on permissions for this appliance, click **User Permissions**.
5. To give an administrator single sign-on permissions, mark the check box next to the user name in the Available users list, and then click the right arrow (>) to add the administrator to the Users with access list.

   Note
   Global Security Administrators and administrators with full appliance access are greyed out in the Users with access list, because they have single sign-on access by default, and this cannot be changed.

6. Click **Save**.

An appliance can only be configured for single sign-on from one TRITON Management Server. If another TRITON instance has already registered an appliance with single sign-on, an error message appears. Select **Transfer registration** to transfer the single sign-on to this instance of TRITON Manager, or select **Register without Single Sign-On** to register the appliance and preserve single sign-on configuration on the other TRITON Management Server.

4 Backup and Restore of TRITON Data

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

You can back up your TRITON Manager settings and system data on your TRITON Management Server machine, and revert to a previous configuration if required. Data saved by the backup process can also be used to import configuration information after an upgrade, and to transfer configuration settings to a different TRITON Management Server machine.

> **Important**
> Make sure that all administrators log off from TRITON Manager before you back up or restore your configuration.

The backup process saves:

- Global configuration and infrastructure information, including administrator and appliance data, stored in the TRITON Settings Database.
- Certificate files required for the TRITON browser components.

The backup process works as follows:

1. You initiate an immediate backup (see *Running immediate backups*, page 41) or define a backup schedule (see *Scheduling TRITON infrastructure backups*, page 40).
   - Manually launch a backup at any time.
   - Backup files are stored in the **C:\EIPBackup** directory by default. To change the backup file location, see *Changing backup settings*, page 42.
2. The backup process checks all TRITON infrastructure components on the machine, collects the data eligible for backup, and creates a new folder in the EIPBackup directory with the format:

   ```
   mm-dd-yyyy-hh-mm-ss-PP
   ```

   This format represents the date and time of the backup, for example:

   ```
   02-10-2011-10-45-30-PM
   ```

   Each backup folder contains a number of files, including:
   - EIP.db: a standard PostgreSQL backup file.
   - httpd-data.txt: contains embedded certificate information and encryption keys

- backup.txt: created if the backup completes successfully
- DataBackup.log: a detailed log file containing information generated during backup

These files should be part of your organization's regular backup procedures.

To check that a backup completed successfully, navigate to the **C:\Program Files (X86)\Websense\EIP Infra** directory and open the **EIPBackup.log** file in a text editor such as Notepad. The log information should look similar to this:

```
2/15/2011 2:27:42 AM --- Backing up to: C:\EIPBackup\2-15-
2011-2-27-42-AM
2/15/2011 2:27:42 AM --- Backing Up Certificates ...
2/15/2011 2:27:42 AM --- Backing Up PostgreSQL ...
2/15/2011 2:27:42 AM *** BACKUP FINISHED ***
```

Each TRITON module has its own backup and restore process for the module system settings:

- For the Data module, see Backing up the system in TRITON AP-DATA Help.
- For the Email module, see Backing up and restoring management server settings in TRITON AP-EMAIL Help.
- For the Web module, see Backing up and restoring your web protection software.

You should run TRITON infrastructure backups in synchronization with TRITON AP-WEB backups. See *Synchronizing TRITON infrastructure and TRITON AP-WEB backups*, page 43.

Scheduling TRITON infrastructure backups

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

When you installed TRITON Manager, a scheduled task for backups was created. By default this task is disabled.

Notify TRITON administrators of the backup schedule, so that they can be sure to log off from TRITON Manager during the backup process.

All backups are "hot"—that is, they do not interfere with system operation. However, Forcepoint recommends that you schedule backups when the system isn't under significant load.

To schedule backups on Windows Server 2008:

1. On the TRITON Management Server, go to **Start > Administrative Tools > Task Scheduler**.
2. In the Task Scheduler window, select **Task Scheduler Library**.
3. Right-click the **Triton Backup** task and select **Enable**.
4. Right-click **Triton Backup** again and select **Properties**.

5. Select the **Triggers** tab.
6. Click **Edit**, and edit the schedule as required. By default, the task is scheduled to run weekly on Saturdays at midnight.
7. Click **OK** twice.
8. If requested, enter your administrator password for the TRITON Management Server machine to confirm the changes to the task.

Running immediate backups

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

Before running a manual backup, make sure that all administrators are logged off from TRITON Manager.

To launch an immediate backup:

1. On the TRITON Management Server, go to **Start > Administrative Tools > Task Scheduler**.
2. In the Task Scheduler window, select **Task Scheduler Library**.
3. If the **Triton Backup** task is disabled, right-click the task and select **Enable**.
4. Right-click the **Triton Backup** task and select **Run**.

Restoring TRITON infrastructure backup data

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

You can activate the restore operation from the TRITON Infrastructure Modify wizard. Make sure that all administrators are logged off from TRITON Manager.

Before starting the restore process, it is recommended that you stop the TRITON Manager service.

To restore TRITON infrastructure data:

1. On the TRITON Management Server, go to **Start > Administrative Tools > Services**.
2. Right-click the **Websense TRITON Manager** service and select **Stop**.
3. Open the Windows Control Panel and select **Programs > Programs and Features**.
4. Select **Websense TRITON Infrastructure**.
5. Click **Uninstall/Change**.
6. When asked if you want to add, remove, or modify the TRITON Infrastructure, select **Modify**.
7. Click **Next** until you get to the **Restore Data from Backup** screen.

8. Select **Use backup data**, then click **Browse** to locate the backup folder.
9. Click **Next** until you begin the restore process.
10. Click **Finish** to complete the restore wizard.
11. Go back to the Services window and click **Refresh**. If the **Websense TRITON Manager** service has not restarted, right-click it and select **Start**.

Once the restore process is complete, a file named **DataRestore.log** is created in the date-stamped backup folder that was used for the restore.

Changing backup settings

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

When you run your first backup, an **EIPBackup** directory is created to contain the date-stamped folders for each set of backup files. By default this directory is created in C:\. You can change this location, and also define how many old backups are kept in the backup directory.

To change the settings for the backup files:

1. On the TRITON Management Server, navigate to the **C:\Program Files (X86)\Websense\EIP Infra** directory.
2. Open **EIPBackup.xml** in a text editor such as Notepad.

   This file contains the following parameters:

Parameter	Description
NUM_OF_COPIES	The number of old backups to store in the backup directory. Defaults to 5.
PATH	The location of the EIPBackup directory. Defaults to C:\.
DOMAIN	Only required if the <PATH> parameter is set to access a remote machine and you need to supply credentials in the form domain\user to write to the location. Leave this field blank if you have defined a path on the local machine, or if you have entered credentials in <USER_NAME>.
USER_NAME	Only required if the <PATH> parameter is set to access a remote machine and you need to supply a user name to write to the location. Leave this field blank if you have defined a path on the local machine, or if you have entered credentials in <DOMAIN>.
PASSWORD	Only required if the <PATH> parameter is set to access a remote machine and you have entered credentials in either <DOMAIN> or <USER_NAME>. Passwords are stored as plain text.

3. Edit the <NUM_OF_COPIES> parameter to specify the number of old backups that should be kept. Once this number is reached, the oldest backup is deleted when the next backup is run.
4. Edit the <PATH> parameter to define the location of the backup files. The location must exist already as the backup process will not create it. For example, if you set the parameter to a location on the TRITON Management Server machine, such as:

   ```
   <PATH>D:\TRITON\Backups</PATH>
   ```

   the backup files will be stored in D:\TRITON\Backups\EIPBackup.

   You can also set the location to be another machine on your network, for example:

   ```
   <PATH>//server01/backups</PATH>
   ```

   If you do this, you may also need to enter credentials for access to the remote machine in the <USER_NAME> or <DOMAIN>, and <PASSWORD> parameters. This is not recommended as the password is stored as plain text and could therefore be accessed by other users. Instead, it is recommended that you store the backups in a location to which you have write access without needing credentials.

   Note
   If you change the location of the backup files, older backup files are deleted only from the new location. Manage backup files in any previously-defined locations manually.

5. Save the file when done. Changes take effect when the next backup is run.

Synchronizing TRITON infrastructure and TRITON AP-WEB backups

TRITON Manager Help | Web, Data, and Email Protection Solutions | v8.2.x

If you have the Web module, administrator information, including permissions and local administrators' passwords, is stored in both the TRITON Settings Database and the Web Security Policy Database. This is because the administrators defined on the **TRITON Settings > Administrators** page can then be assigned roles in the Web module, and different privileges within those roles.

To ensure that this information is kept in sync, always back up and restore TRITON AP-WEB and the TRITON infrastructure at the same time. The steps in this section describe the TRITON infrastructure backup followed by the TRITON AP-WEB backup; however, the order in which you run the two processes does not matter, as long as there are no changes made in TRITON Manager for the duration of both backups.

To run a combined TRITON AP-WEB and TRITON Infrastructure manual backup:

1. Follow the instructions in *Running immediate backups*, page 41.

2. Open a command prompt and navigate to the **bin** directory (by default C:\Program Files (X86)\Websense\Web Security\bin).
3. Enter the following command:

   ```
   wsbackup -b -d <directory>
   ```

   Here, *directory* indicates the destination directory for the Web backup archive.

To schedule a combined TRITON AP-WEB and TRITON Infrastructure backup, set the schedule time and frequency to ensure the backups are always synchronized. Follow the instructions in *Scheduling TRITON infrastructure backups*, page 40, then see "Scheduling backups" in TRITON AP-WEB Help.

To run a combined TRITON AP-WEB and TRITON Infrastructure restore:

1. On the TRITON Management Server, go to **Start > Administrative Tools > Services**.
2. Right-click the **Websense TRITON Manager** service and select **Stop**.
3. Right-click the **Websense Web Security** service and select **Stop**.
4. Follow the TRITON Infrastructure restore process in *Restoring TRITON infrastructure backup data*, page 41.
5. Run the backup utility in restore mode, as described in Restoring your web protection configuration in the TRITON Backup and Restore document. Ensure the backup file you specify has the same date as the TRITON infrastructure backup file.
6. Go back to the Services window and click **Refresh**. If the Web Security service has not restarted, right-click it and select **Start**.