



Forcepoint DLP

10.0

Forcepoint Security Manager Help

© 2023 Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.

Published 25 January 2023

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Contents

| | |
|---|----|
| 1 Getting Started | 5 |
| Logging on to the Security Manager..... | 6 |
| Navigating the Security Manager..... | 11 |
| Using the Forcepoint Support Portal..... | 12 |
| 2 Configuring Global Settings | 13 |
| Viewing your account information..... | 14 |
| Setting user directory information..... | 15 |
| Introducing administrators..... | 17 |
| Enabling access to the Security Manager..... | 19 |
| Setting email notifications..... | 27 |
| Configuring two-factor authentication..... | 29 |
| Global Settings audit log..... | 36 |
| 3 Accessing Appliances | 39 |
| Managing appliances..... | 39 |
| 4 Backup and Restore of Global Settings Data | 45 |
| Scheduling management infrastructure backups..... | 46 |
| Running immediate backups..... | 47 |
| Restoring management infrastructure backup data..... | 48 |
| Changing backup settings..... | 49 |

Chapter 1

Getting Started

Contents

- Logging on to the Security Manager on page 6
- Navigating the Security Manager on page 11
- Using the Forcepoint Support Portal on page 12

Applies to:

- Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x
- Forcepoint DLP v8.5.x, v8.6.x, v8.7.x, v8.8.x, v8.9.x, v9.0, v10.x
- Forcepoint Email Security, v8.5.x
- Forcepoint appliances, v8.5.x

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

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

- The Web Security module allows Forcepoint Web Security and Forcepoint URL Filtering administrators to develop, monitor, and enforce Internet access policies.
- The Data Security module allows Forcepoint DLP administrators to create policies that protect organizations from information leaks and data loss at the perimeter and inside the organization.
- The Email Security module allows Forcepoint Email Security administrators to protect their organization against the threats of malware, spam, and other unwanted content in email traffic.

If your subscription includes Forcepoint Mobile Security, the Security 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 Security Manager, browse this guide or select one of the following topics as a launch point.

| First steps | Manage administrators |
|---|---|
| <ul style="list-style-type: none">■ <i>Logging on to the Security Manager</i>■ <i>Navigating the Security Manager</i>■ <i>Using the Forcepoint Support Portal</i> | <ul style="list-style-type: none">■ <i>Viewing your account information</i>■ <i>Setting user directory information</i>■ <i>Introducing administrators</i>■ <i>Enabling access to the Security Manager</i>■ <i>Setting email notifications</i> |
| Other administrator tasks | Backup and restore |
| <ul style="list-style-type: none">■ <i>Configuring two-factor authentication</i>■ <i>Global Settings audit log</i>■ <i>Managing appliances</i> | <ul style="list-style-type: none">■ <i>Scheduling management infrastructure backups</i>■ <i>Restoring management infrastructure backup data</i> |

Related concepts

[Logging on to the Security Manager](#) on page 6
[Navigating the Security Manager](#) on page 11
[Using the Forcepoint Support Portal](#) on page 12
[Introducing administrators](#) on page 17
[Enabling access to the Security Manager](#) on page 19
[Managing appliances](#) on page 39

Related tasks

[Setting user directory information](#) on page 15
[Viewing your account information](#) on page 14
[Setting email notifications](#) on page 27
[Configuring two-factor authentication](#) on page 29
[Global Settings audit log](#) on page 36
[Scheduling management infrastructure backups](#) on page 46
[Restoring management infrastructure backup data](#) on page 48

Logging on to the Security Manager

The Forcepoint Security Manager is the central configuration interface used to manage software configuration and settings for Forcepoint software modules. This web-based tool runs on a variety of popular browsers (see the [Certified Product Matrix](#) for details).

Although it is possible to launch the Security Manager using non-supported browsers, the application may not display properly and some features may not appear.

For more information, refer the related topics given below:

- [Logging on with RSA SecurID authentication](#)
- [Logging on with certificate authentication](#)
- [Security certificate alerts](#)
- [Security Manager session timeouts](#)

Related concepts

[Security certificate alerts](#) on page 9
[Security Manager session timeouts](#) on page 9

Related tasks

[Logging on with RSA SecurID authentication](#) on page 8
[Logging on with certificate authentication](#) on page 8

Security Manager requirements

- The Security Manager frequently uses pop-up dialog boxes for user interaction. Be sure to disable pop-up blockers before accessing the Security Manager.

Launching the Security Manager

To open the Security Manager, do one of the following:

- On Windows machines, launch **Forcepoint Security Manager** from the Start screen or **Start > All Programs > Forcepoint**.
- Double-click the **Forcepoint Security 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/
```

Substitute the IP address or hostname of the management server machine. It is recommended that you use the IP address, particularly when launching Security Manager from a remote machine.

After installation, the default user, **admin**, has full administrative access to all Security Manager 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 an administrator **User name** and **Password**, then click **Log On**. If your organization is using two-factor authentication, see *Logging on with certificate authentication*.



Note

When a local administrator account created in the Security Manager has the same credentials as a network account (same user name and password), the local account takes precedence.

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

Related tasks

[Logging on with certificate authentication](#) on page 8

Logging on with RSA SecurID authentication

Before you begin

The process of logging in with RSA® SecurID is described in *How RSA SecurID authentication works*.

If RSA SecurID authentication is enabled, and administrators encounter an issue in which authentication is failing, it is still possible to log on to the Security Manager as follows:

Steps

- 1) Open a browser on the Forcepoint management server machine (for example, via a Remote Desktop Connection).
- 2) Go to the URL <https://127.0.0.1:9443/> (or <https://localhost:9443/>).
- 3) Log on using the **admin** user name and password.

Next steps

Next, configure the RSA SecurID authentication options to provide a fallback for other administrators (see *Configuring two-factor authentication*).

Related tasks

[How RSA SecurID authentication works](#) on page 31

[Configuring two-factor authentication](#) on page 29

Logging on with certificate authentication

Before you begin

When certificate authentication is enabled, the process works as described in *How certificate authentication works*.

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

Steps

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

Next steps

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

If all administrator accounts are configured to use certificate authentication, and an issue arises in which administrators do not have client certificates or certificate matching is failing, it is possible to log on to the Security Manager as follows:

- 1) Open a browser on the Forcepoint management server machine (for example, via a Remote Desktop Connection).
- 2) Go to the URL <https://127.0.0.1:9443/> (or <https://localhost:9443/>).
- 3) Log on using the **admin** user name and password.

Next, configure certificate authentication options to provide a fallback for other administrators (see *Configuring two-factor authentication*).

Related tasks

[How RSA SecurID authentication works](#) on page 31

[Configuring two-factor authentication](#) on page 29

Security certificate alerts

An SSL connection is used for secure, browser-based communication with Security 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 displays when the Security Manager is launched from a new browser. To avoid seeing this error, install or permanently accept the certificate within the browser.

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



Note

If you are using Internet Explorer, the certificate error remains present after you accept the certificate. Close and reopen your browser to remove the error message.

Security Manager session timeouts

A Security Manager session ends 22 minutes after the last action taken in the user interface (for example, clicking from page to page, entering information, caching changes, or saving changes). A warning message is displayed two minutes before the session ends.

- Any uncached or unsaved changes are lost when the session ends. Remember to save and deploy changes regularly.
- If the Security 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 the Security Manager is open in multiple browser windows on the same computer, the instances share the same session by default. If the session times out in one window, it times out in all windows.
- To open multiple Security Manager instances that do not share a session, open each instance in a different browser (for example, Internet Explorer and Chrome). In this situation, if one window times out, the others are not affected.

If an administrator closes the browser without logging off from the Security Manager, or if the remote machine from which the Security Manager is being accessed shuts down unexpectedly, the administrator account may be temporarily locked out. The software typically detects this issue within about two minutes and ends the interrupted session, allowing the administrator to log on again.

If the administrator has multiple browsers running in this scenario, they 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 session and allow a new logon within two minutes.

Configuring encrypted connection to SQL Server

Before you begin

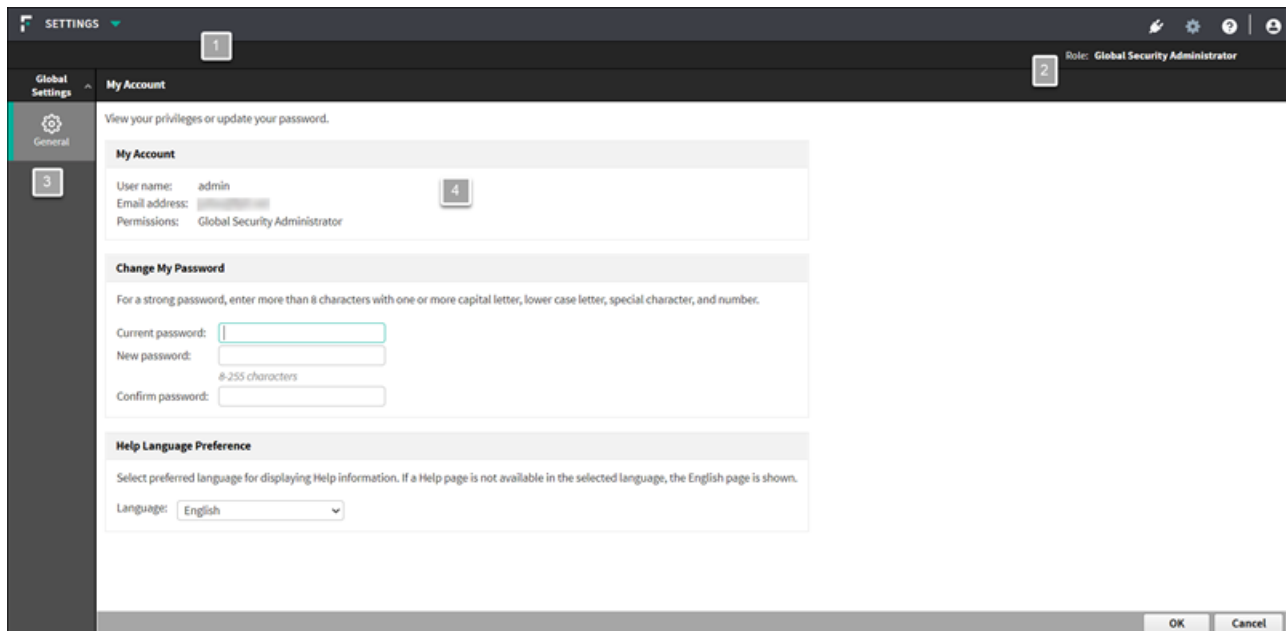
Forcepoint Security Manager communicates with your organization's SQL Server database. It is recommended to implement SSL encryption for these communications to increase the level of security in the SQL database. Use the following steps to enable the encrypted connection.

Steps

- 1) From the Windows Start menu, click **Forcepoint Security Setup**.
The Forcepoint Security Setup Installer Dashboard displays. The Installer Dashboard stays on-screen during installation. Various subinstallers and dialog boxes are displayed over it.
- 2) From Forcepoint Management Infrastructure, click **Modify**.
The Forcepoint Management Infrastructure Setup wizard displays.
- 3) Click **Next** on the Welcome and Installation Directory screens.
- 4) On the SQL Server screen, mark the check box **Encrypt connection** and click **Next**.
- 5) Complete the Forcepoint Management Infrastructure Setup wizard and click **Finish**.
If you have additional Forcepoint products installed, they must also be modified. All installed products display on the Forcepoint Security Setup Installer Dashboard.
- 6) From Forcepoint Web Security, Forcepoint DLP, or Forcepoint Email Security, click **Modify**.
The relevant setup wizard displays.
- 7) Repeat steps 3–5 for each Forcepoint product.
- 8) On the Forcepoint Security Installer Dashboard, click **Close**.

Navigating the Security Manager

The Global Settings interface can be divided into four main areas. The following image displays the interface for Security Manager version 8.5.3 and later:



- 1) Security Manager toolbar
- 2) Module toolbar
- 3) Navigation pane
- 4) Content pane

The **Security Manager toolbar** shows:

- The User Details drop-down list, which shows the current logged-on account and provides a Log Off button to end the administrative session
- Icons used to configure appliances and global settings, and to open Help
- Which module is active
- Use the Module drop-down list in the Security Manager toolbar to switch between modules.
- When administrators log on to the Security Manager, the module they last accessed is active indicated by a green icon in the Module drop-down list.

The **module toolbar** contains information and options relevant to the Security Manager module that is currently active. For the Global Settings or Appliances pages, it shows the current administrator account.

The **navigation pane** contains the available navigation choices for the current Security Manager module or configuration option.

The **content pane** varies according to the selection in the navigation pane. For more information about specific modules, see:

- [Forcepoint DLP Administrator Help](#)
- [Forcepoint Email Security Administrator Help](#)

- [Forcepoint Web Security Administrator Help](#)

Using the Forcepoint Support Portal

Forcepoint maintains a customer support portal, the Forcepoint Hub, at support.forcepoint.com. Use the **Create Account** links to create a support account that can be used to access product updates, patches and hotfixes, product news, evaluations, and technical support resources.

- When you create an account, the account is associated with your organization's 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 an organization can create accounts associated with the same subscription key.

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

- A searchable knowledge base of articles and documents
- Webinars and show-me videos
- Answers to frequently asked questions

For additional questions, click the **Contact Support** link in the toolbar near the top of the page.

- The contact page includes information for finding solutions, opening an online support case, and calling Forcepoint Technical Support.
- For telephone requests, please have ready:
 - Forcepoint subscription key
 - Access to the management console for your solutions (for example, Security Manager and 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

Chapter 2

Configuring Global Settings

Contents

- [Viewing your account information](#) on page 14
- [Setting user directory information](#) on page 15
- [Introducing administrators](#) on page 17
- [Enabling access to the Security Manager](#) on page 19
- [Setting email notifications](#) on page 27
- [Configuring two-factor authentication](#) on page 29
- [Global Settings audit log](#) on page 36

Use the Forcepoint Security Manager to manage Forcepoint Web Security, Forcepoint DLP, and Forcepoint Email Security configuration, policies, and reporting from a central management console.

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

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

See *Introducing administrators*.



Note

Changes to Global Settings (such as new administrator accounts) can take between 30 and 90 seconds to propagate to other Security Manager modules.

Global Settings can also be used to:

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

Related concepts

[Introducing administrators](#) on page 17

Related tasks

- [Setting email notifications on page 27](#)
- [Viewing your account information on page 14](#)
- [Setting user directory information on page 15](#)
- [Configuring two-factor authentication on page 29](#)
- [Global Settings audit log on page 36](#)

Viewing your account information

Before you begin

Use the page **Global Settings > General > My Account** to view permissions information for your administrator account and select a language other than English as your preferred Help language. If you have been assigned a local user name and password for the Security Manager, you can also change your password on this page.

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

The toolbar at the top of the page displays the permissions allocated to your account:

Steps

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

Next steps

To change your password:

- 1) In the section Change My Password, 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).
 - Click **OK**.
The changes are saved.

To change the Help language:

- 1) In the section Help Language Preference, select an entry in the drop-down list **Language**.
- 2) Click **OK**.

The changes are saved.

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.

Related concepts

[Global Security Administrator](#) on page 17

Setting user directory information

Before you begin

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

Steps

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

Next steps

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

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

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

- Duplicate user names are not supported in an LDAP-based directory service. Ensure that the same user name does not appear in multiple domains.
- With 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 the Security Manager using a network account:

- 1) Select a user directory type from the drop-down list **User directory server**; **Active Directory**, **Generic Directory**, **Lotus Notes**, **Novell eDirectory**, or **Oracle Directory Server**.

Configuration options display for your selection.

- 2) Enter the **IP address or host name** to identify the directory server.
- 3) Enter the communication **Port** for the directory.
- 4) Enter a **User distinguished name** and **Password** for the administrative account that 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.
 - In the field **User distinguished name**, enter the account details as a single string. You can use the format “CN=user, DC=domain” or, if your organization uses Active Directory, “domain\username”.
- 5) 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, click **Test Connection**.
- 6) Enter the **Root naming context** that the Security 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 the 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 the LDAP schema includes nested groups, mark the check box **Perform additional nested group search**.
- 8) To encrypt communication with the directory service, mark the check box **Use SSL encryption**.
- 9) If the directory service uses LDAP referrals, mark the check box to indicate whether the software should follow the referrals.
- 10) For Generic Directory, configure the following additional 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 distinguished name of the user.
- 11) Click **OK**.

The settings are saved.



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

The page **Global Settings > General > Administrators** is used to create and manage the accounts that administrators use to access the Security Manager.

Administrators can access the Security 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 Security Manager modules. See *Global Security Administrator*.
- Other types of administrators have more restricted access to Security Manager modules. An administrator may be given permission to manage or audit one or more Security Manager modules using the same account. See *Security Manager administrators*.

Administrators can be identified using either network logon credentials or local accounts used only for the Security Manager. See *Adding a network account*, and *Adding a local account*.

Related concepts

[Global Security Administrator](#) on page 17

[Security Manager administrators](#) on page 18

Related tasks

[Adding a network account](#) on page 22

[Adding a local account](#) on page 20

Global Security Administrator

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 the Security Manager, and also the following permissions in the modules that are part of your subscription:

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

**Note**

In deployments that include Forcepoint appliances, access to the command-line interface (CLI) is controlled with a separate password.

The permissions given to a Global Security Administrator within the individual Security Manager 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 additional Global Security Administrators as needed. Creating multiple Global Security Administrators ensures that if the primary Global Security Administrator is not available, another administrator can access all Security Manager policy and configuration settings.

Security Manager administrators

When a Security Manager administrator account is created, the administrator is given access to one or more Security Manager modules.

Administrators can be given either simple “access” or “access and account management” permissions for a module. By default, the following permissions are allocated:

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

Administrator permissions can be changed in the Web Security module on the page **Policy Management > Delegated Administration**.

- For the Data Security module, regardless of which option is selected, the administrator is assigned the Default access role, with access to the pages **Incidents & Reports, Dashboard, and My Settings**. Administrator permissions can be changed in the Data Security module on the pages **Settings > Authorization > Administrators** and **Settings > Authorization > Roles**.
- **Email Security 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 Security module on the page **Settings > Administrators > Delegated Administrators**.

Administrators with account management permissions can also edit and delete other administrator accounts in the Security Manager, subject to the limitations of their permissions.

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

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

Related tasks

[Viewing your account information](#) on page 14

Enabling access to the Security Manager

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



Note

This page is available only to Global Security Administrators and administrators who have permission to manage at least one Security Manager 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 Security Manager modules.

Next to the Name column, the Administrator type column (new in version 8.6.3) displays the type of administrator:

- The **User** type is used for all administrator accounts that require access to the Security Manager. This is the standard role for all administrators accounts.
- The **Application** type is used to access REST API services in the Data Security module. The Application type provides permissions to perform API requests to the Security Manager. This type is not supported for administrators with permissions on the Web or Email modules.

Next to the Administrator type column, the Account type column displays the type of account:

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

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



Note

If RSA SecurID authentication is enabled on the page **General > Two-Factor Auth**, any administrator accounts with a User type added on this page are used only as a fallback if the RSA Authentication Manager cannot be reached.

RSA SecurID is not supported for the Application type. See *Configuring two-factor authentication*.

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 Security Manager administrator with permission to manage at least one Security Manager 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 Forcepoint DLP 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 Security module.

Related tasks

[Setting email notifications on page 27](#)

[Adding a local account on page 20](#)

[Adding a network account on page 22](#)

[Configuring two-factor authentication on page 29](#)

Adding a local account

Next steps

To add local administrator accounts:

- 1) Navigate to the page **Global Settings > General > Administrators** and click **Add Local Account**. The Add Local Account page displays.
- 2) Enter a unique **Name**.
 - The name must be between 1 and 50 characters long, and cannot include any of the following characters:
* < > ' ' { } ~ ! \$ % & @ # . " | \ & + = ? / ; : , ^ ()
 - Names can include spaces and dashes.
- 3) Enter a valid **Email address** for the user.
This email address is used to send account information to the new administrator.
- 4) Enter and confirm a **Password** for this user.
The password must be 8–255 characters and include at least one of 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 page **General > Two- Factor Auth**, password logon is not available for the local account.

- 5) Under **Administrator type**, select either **User** or **Application**. ([Added version 8.6.3](#))
 - Select **User** for administrator accounts that require access to the Security Manager. This is the standard type for all administrators.
 - Select **Application** if the account is used to access REST API services in the Data Security module. The Application type provides permissions to perform API requests to the Security Manager. The Email Address provided for this account will be used as the Application owner's contact. Forcepoint DLP uses this email address if there is an issue with the Application.

If you select **Application**, then all module access permission options on this page are disabled. The Application type grants access to the Data module by default and grants no permissions to the other

modules. These permissions cannot be edited. Also, the **Notify administrator of the new account via email** and **Force administrator to create a new password at logon** options are not available.

- 6) To create an administrator with full permissions across all Security Manager modules and functions, mark the check box **Global Security Administrator**.



Note

Only Global Security Administrators can create other Global Security Administrators.

- 7) To send account information and access instructions to the new administrator via email, mark the check box **Notify administrator of the new account via email**.
To send administrator emails, you must set up SMTP details on the Notifications page. Optionally, also customize the contents of the email message on the Notifications page (see *Setting email notifications*).
- 8) To require the administrator to change the account password the first time he or she logs on to the Security Manager, mark the check box **Force administrator to create a new password at logon**.
- 9) If certificate authentication is enabled on the page **General > Two-Factor Authentication**:
- 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*.

- 10) If this account is not a Global Security Administrator, in the section Module Access Permissions, select the permissions 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 Security Manager 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 *Security Manager administrators*.



Note

Administrators can assign access permissions only for the Security Manager modules for which they have management permissions.

- 11) When you are finished making changes, click **OK**.
The changes are saved.

Related topics are listed below:

- *Enabling access to the Security Manager*
- *Adding a network account*
- *Editing a local account*

Related concepts

[Enabling access to the Security Manager on page 19](#)

[Security Manager administrators on page 18](#)

Related tasks

[Adding a network account on page 22](#)

[Editing a local account on page 24](#)

[Setting email notifications on page 27](#)

[Configuring two-factor authentication on page 29](#)

Adding a network account

Before you begin

Next steps

To add users defined in a supported directory service as Security Manager administrators:

- 1) Navigate to the page **Global Settings > General > Administrators** and click **Add Network Account**.
- 2) In the field **Search**, enter keywords to search on to find the accounts to add as Security Manager administrators. By default, the search query already includes a wildcard so there is no need to include an asterisk (*) in a search.
By default, the search context for your search is the default domain context from the Directory Service page (see *Setting email notifications*). To edit this context, click **Refine search** and enter a new search context. To revert to the default context, click **Restore default**.

For users, the following attributes are searched in the selected context.

- **Active Directory:** Email Address, Logon Name, and Display Name
- **Novell eDirectory, Oracle Directory Service, or Lotus Notes/Domino:** Email, Display Name, Username, and Common Name (CN)
For groups, the CN field is searched for all directory services.

Search results display in the **Search results** list on the left-hand side. The search results list both users and groups that match the specified keywords, and that include both user name and email address in the directory service.

- 3) To add a user or group as an administrator, mark the check box next to the account name in the **Search results** list, then click the right arrow (>) to add the account to the **Selected accounts** list.
To remove a user from the **Selected accounts** list, mark the check box next to the account name, then click the left arrow (<).
- 4) If certificate authentication is enabled on the page **General > Two-Factor Auth** (see *Configuring two-factor authentication*), click **Certificate Authentication** to upload or import the certificate used to authenticate the selected administrators during Security 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 display in the **Certificate Authentication** section of the page.

- 5) Once you have added one or more accounts to the **Selected accounts** list, mark the check box to 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*).

- 6) Next, select the access permissions for the new administrators.

- Mark the check box **Global Security Administrator** to create an administrator with full permissions across all Security Manager modules.



Note

Only Global Security Administrators can create other Global Security Administrators.

- If the accounts are not Global Security Administrators, in the section **Module Access Permissions**, select permissions for 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 Security Manager 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 *Security Manager administrators*.



Note

Administrators can assign access permissions only for the Security Manager modules for which they have management permissions.

- 7) After configuring administrator accounts, click **OK**. The settings are saved.

Related concepts

[Security Manager administrators](#) on page 18

Related tasks

[Setting email notifications](#) on page 27

[Adding a local account](#) on page 20

[Editing a network account](#) on page 26

[Configuring two-factor authentication](#) on page 29

Editing a local account

Before you begin

Use the page **Global Settings > General > Administrators** to edit the access and authentication permissions for existing local accounts.

Steps

- 1) From the page **Administrators**, click the name of an administrator account.
The **Edit Local Account** page displays.
- 2) To change the name, enter a unique name up to 50 characters in the field **Name**.
 - The name must be between 1 and 50 characters long, and cannot include any of the following characters:
* < > ' { } ~ ! \$ % & @ # . " | \ & + = ? / ; : ,
 - Names can include spaces and dashes.
- 3) To change the administrator email address, enter a valid address for the user in the field **Email address**.
This email address is used to send account information to the administrator.
- 4) To reset the administrator's password, enter and confirm a password in the fields **Change password** and **Confirm password**.
The password must be 8–255 characters and 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 page **General > Two- Factor Auth**, password logon is not available for the local account.

- 5) Under **Administrator type**, select either **User** or **Application**. ([Added in version 8.6.3](#))
 - Select **User** for administrator accounts that require access to the Security Manager. This is the standard type for all administrators.
 - Select **Application** if the account is used to access REST API services in the Data Security module. The Application type provides permissions to perform API requests to the Security Manager. The Email Address provided for this account will be used as the Application owner's contact. Forcepoint DLP uses this email address if there is an issue with the Application.

If you select **Application**, then all module access permission options on this page are disabled. The Application type grants access to the Data module by default and grants no permissions to the other modules. These permissions cannot be edited. Also, the **Notify administrator of the new account via email** and **Force administrator to create a new password at logon** options are not available.

- 6) To give the administrator full permissions across all Security Manager modules, mark the check box **Global Security Administrator**.

**Note**

Only Global Security Administrators can create other Global Security Administrators.

- 7) To send account update information to the administrator via email, mark the check box **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.

- 8) To require the administrator to change the account password the next time they log on to the Security Manager, mark the check box **Force administrator to create a new password at logon**.
- 9) If certificate authentication is enabled on the page **General > Two-Factor Auth**:
- Click **Certificate Authentication**.
 - Browse to the location of the certificate that the administrator will authenticate against when logging on to the Security Manager.
 - Click **Upload Certificate**.

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

- 10) If this is not a Global Security Administrator account, use the section **Module Access Permissions** 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 Security Manager modules.

For each available 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 *Security Manager administrators*.

**Note**

Administrators can assign access permissions only for the Security Manager modules to which they have management permissions.

- 11) When you are finished making changes, click **OK**.
The settings are saved.

Related concepts

[Security Manager administrators](#) on page 18

Related tasks

Configuring two-factor authentication on page 29

Editing a network account

Before you begin

Use the page **Global Settings > General > Administrators** to edit the access and authentication permissions for existing network accounts

Steps

- 1) On the page Administrators, click an account name.
The Edit Network Account page displays.
- 2) If certificate authentication is enabled on the page **General > Two-Factor Auth** (see *Configuring two-factor authentication*), click **Certificate Authentication** to upload or import the certificate that the administrators will authenticate against when logging on to the Security 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. To import a new certificate from your user directory, replacing the existing certificate, click **Import New from LDAP**.

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

3) To change the access permissions for the network account:

- Select **Global Security Administrator** to give the administrator full permissions across all Security Manager modules.



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 Security Manager modules.

For each available 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 *Security Manager administrators*.



Note

Administrators can assign access permissions only for the Security Manager modules to which they have management permissions.

4) When you are done editing administrator permissions, click **OK**.
The settings are saved.

Related concepts

[Security Manager administrators](#) on page 18

Related tasks

[Configuring two-factor authentication](#) on page 29

Setting email notifications

Use the page **Global Settings > General > Notifications** to set up the mail server used for all email notifications from the Security Manager, and to configure the notification email messages sent to administrators.



Note

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

To establish a connection with a mail server so that email notifications can be sent:

- 1) Enter the **Sender email address** to use in notifications. If you are using Exchange Online, a valid email address must be used.

- 2) 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 the Forcepoint Security Manager.
- 3) Select the **Mail server type**.
 - If you select **Exchange Online**:
 - a) Enter the applicable **Tenant ID**, **Client ID**, and **Client secret**. For more information about getting your Tenant ID, Client ID, and Client secret, see the [Configuring Azure Active Directory to use OAuth2 authentication](#) Knowledge Base article.
 - b) Click **Test Connection** to test the outgoing mail server settings. When prompted, enter an email address where the system can send a test message. If you receive the message, then it was able to connect to the outgoing mail server successfully. This can take several minutes.
 - If you select **Other mail server**, enter the **IP address or host name** and **Port** of the SMTP server machine.
- 4) Next, in the section Email Notification Templates, review the templates used for administrator notifications. There are three available templates:
 - **New Account**: Notifies an administrator of their new Security Manager 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 Security Manager 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 Security Manager 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 can be used or modified, 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:

- a) Select one of the Email Notification Templates tabs: **New Account**, **Edit Account**, or **Forgot Your Password**.
- b) Enter a suitable subject header for the email message. For example, for a new account, you might use “Welcome to Forcepoint Security Manager” or “Your new Forcepoint Security Manager account.”
- c) 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 the Security Manager. |
| %Username% | The administrator’s Security Manager name. |

| Variable | Description |
|---------------|---|
| %Password% | The administrator's Security Manager 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.

- d) To return to the default notification text at any time, click **Restore Default**, then click **OK** to confirm.
- 5) Click **OK**.
The settings are saved.

Configuring two-factor authentication

Use the page **Global Settings > General > Two-Factor Auth** 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 two forms of identification when logging on to the Security Manager.

Access to Forcepoint Mobile Security is not covered by two-factor authentication; you must log on to the cloud-based console using your regular user name and password.

The following methods are available:

- RSA SecurID® authentication (see *How RSA SecurID authentication works*).
- Certificate authentication (see *How certificate authentication works*). If you choose to enable RSA SecurID authentication:
 - Use RSA Authentication Manager 6.1.2 or higher.
 - Create a custom agent for the Forcepoint Security Manager in the RSA Authentication Manager (see *Creating a custom agent for RSA SecurID authentication*).
 - Certificate authentication is automatically disabled. If you have previously enabled certificate authentication, and then enable RSA SecurID authentication, a warning message appears.

If your Forcepoint management server has more than one network interface controller (NIC), use the following steps to configure RSA authentication to use the proper IP address for communicating with the RSA Authentication Manager:

- 1) Open **rsa_api.properties** located at **\\Websense\EIP Infra\tomcat\wbsnData\rsaSecurID**.
- 2) Locate the line **RSA_AGENT_HOST=**
- 3) Add the IP address of the server that is configured for the installation:
 - a) **RSA_AGENT_HOST=x.x.x.x**
 - b) **x.x.x.x=IP address for management server**
- 4) Save the **rsa_api.properties** file.
- 5) Restart the **Websense TRITON Unified Security Center** service in

To set up Security Manager RSA SecurID authentication:

- 1) In the section RSA SecurID Authentication, mark the check box **Authenticate administrators using RSA SecurID authentication**.
- 2) Enter a valid **User name** and **Passcode** for RSA SecurID logon.
The user must be able to authenticate with RSA Authentication Manager but does not have to be a Security Manager administrator.
- 3) Click **Test Connection to RSA Manager**.
The connection test must be successful before the Security Manager allows changes to be saved 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*.
- 4) To allow administrators to log on to the Security Manager if RSA authentication is unavailable, mark the check box **Fall back to other authentication mechanisms**.
This means that any administrators configured on the page **General > Administrators** 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.
- 5) Click **OK**.
The settings are saved.

To set up Security Manager certificate authentication:

- 1) In the section Certificate Authentication, mark the check box **Authenticate administrators using client certificate authentication**.
- 2) To enable attribute matching, in the section Certificate Matching, mark the check box **Use attribute matching as a fallback method** and select whether it applies to all administrators or only to administrators without certificates in the Security Manager.
To configure the attributes used for matching, click **Configure Attribute Matching**, then see *Setting up attribute matching*.
- 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 page **General > Administrators > Edit Network Account**.

- 4) In the section Root Certificates, click **Add** to add a root certificate for signature verification. There must be at least one root certificate in the Security Manager for two-factor authentication to operate.
 - Browse to the location of the root certificate file, then click **Upload Certificate**.
- 5) Whenever a root certificate is added or changed, create a new master certificate file and copy it to the “Websense TRITON Web Server” service. Click **Create Master Certificate File** to create the new file, then see *Deploying the master certificate file* for further information.
- 6) In the section Password Authentication, to enable password authentication as a fallback method, mark the check box **Allow password authentication to log on to the Security Manager for:** and select whether it applies to all administrators or only to administrators without certificates in the Security Manager.



Note

The “admin” account created during installation can always log on from the Forcepoint management server machine using password-based authentication.

- 7) Click **OK**.
The settings are saved.

Related concepts

[How certificate authentication works on page 34](#)

[Test connection to RSA Manager results on page 33](#)

Related tasks

[How RSA SecurID authentication works on page 31](#)

[Creating a custom agent for RSA SecurID authentication on page 32](#)

[Setting up attribute matching on page 35](#)

[Deploying the master certificate file on page 34](#)

How RSA SecurID authentication works

Before you begin

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

Steps

- 1) The Security Manager detects that RSA SecurID authentication is enabled and available, and displays the RSA version of the logon screen. (The “Forgot my password” link on this screen does not apply to SecurID passcodes.)

- 2) Administrators provide their two-factor authentication credentials as defined by their organization. For example:
 - The SecurID user name might be the administrator's email address or network logon name.
 - The passcode is usually a PIN combined with a token code supplied by a separate hardware or software token; the format depends on each organization's configuration.
- 3) The authentication mechanism searches the local repository for a user profile that matches the user name provided. If there is no match, the search is repeated in the directory service. If a network user is found, the Security Manager looks for groups that have been assigned permissions in the system, and the RSA logon proceeds if an intersection is found between the groups.
- 4) The Security Manager custom agent checks the SecurID user name and the passcode against the Authentication Manager. If authentication fails, the authentication request falls back to Security Manager 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 may 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

Before you begin

To enable and use RSA SecurID two-factor authentication, first use RSA Authentication Manager to create a custom agent for the Forcepoint Security Manager. This agent is used to communicate with the RSA Authentication Manager server when you test the connection on the page **General > Two-Factor Auth**, and during the logon process.

To create a custom agent:

Steps

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

| | |
|------------------------|--|
| Name | Hostname of the Forcepoint management server. Must resolve to a valid IP address on the local network. |
| Network Address | IP address of the Forcepoint management server. |
| Agent Type | Select Standard Agent. |
| Encryption Type | Select DES. |

- 2) Click Generate Configuration Files.

- Copy the RSA Authentication Manager configuration file (sdconf.rec) to the following directory on the Forcepoint management server:

```
C:\Program Files (x86)\Websense\EIP\tomcat\wbsnData\ rsaSecurID\
```



Note

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

- If a node secret file (securid) exists, copy this file to the above directory as well.
- Make sure no administrators are logged on to the Forcepoint Security Manager.
- On the Forcepoint management server, open the Windows Services tool.
- Right-click the service **Websense TRITON Unified Security Center** and select **Restart**.

Test connection to RSA Manager results

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

The table below provides more information on the other messages that may display.

| Message | Description |
|--|--|
| Connection succeeded. PIN or next token code required for successful logon. | The Security 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, 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. | The Security 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 <i>Creating a custom agent for RSA SecurID authentication</i> to create a custom agent in your RSA Manager. The check box “Authenticate administrators using RSA SecurID authentication” stays in a partially selected state, and you cannot enable RSA SecurID authentication until you have successfully re-tested the connection. |

| Message | Description |
|--|--|
| Connection failed. Verify your configuration settings. | The Security Manager could not connect to your RSA Manager. The check box “Authenticate administrators using RSA SecurID authentication” stays in a partially selected state, and you cannot enable RSA SecurID authentication until you have successfully re-tested the connection. |

Related tasks

[Creating a custom agent for RSA SecurID authentication](#) on page 32

How certificate authentication works

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

- The Security 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 Security 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, the Security Manager receives the client certificate and checks that it matches the signature in the uploaded root CA certificates. If the signature matches, the Security Manager checks for a full match with the certificates that were either uploaded to the Security Manager or imported from the user directory. If a match is found, the administrator associated with the two-factor authentication credentials is logged on.
- If no certificate match is found and attribute matching is configured 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 Security 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

Before you begin

When a new master certificate is created following changes to the root certificate used for certificate authentication, update the “Websense TRITON Web Server” service with the new file. To do this:

Steps

- 1) Go to the Security Manager installation directory (by default C:\Program Files (X86)\Websense\EIP Infra).
- 2) Run the script file **replace_2fa_certificate.bat**.

Next steps

The script file copies the new master certificate file to the “Websense TRITON Web Server” service, then restarts the service.

Setting up attribute matching

Before you begin

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

To configure attribute matching:

Steps

- 1) From the page **Global Settings > General > Two-Factor Auth**, follow the steps under *Configuring two-factor authentication*, to enable certificate authentication.
- 2) In the section Certificate Matching, click **Configure Attribute Matching**.
The Attribute Matching page displays.
- 3) In the section **Administrator Property**, select a property from the administrator user directory to use 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.

- 4) 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

The Verify Administrator Property button appears only if you have configured a user directory in Global Settings and 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 the Security Manager. To change this field at a later date, click **Update Property** to import the new attribute matching value.

- 5) In the **Certificate Property** section, 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 (DN), which defines the entity associated with this certificate.
 - The unique serial number for each certificate issued by a particular Certification Authority (CA).
- 6) Click **OK**.
The configured properties display in the Certificate Matching section on the page **General > Two-Factor Auth**.

Related tasks

[Configuring two-factor authentication](#) on page 29

Global Settings audit log

Use the page **Global Settings > General > Audit Log** 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 |
|------------------|--|
| Action 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 the Security Manager. |
| Role | Role of the administrator. |
| Topic | Topic related to the action. |
| Action Performed | Details of the action. This column may contain variables that are filled in by the system; for example, a logon user name. |
| Details | Specifics about the action performed. |
| Modified Item | Provides a clickable link with details about the modified item. |

To find a specific Audit Log action:

- 1) In the field **Find ID**, enter the ID number of an Audit Log action.
- 2) Click **Find** 
The action displays.
- 3) Show all Audit Log actions, click **Clear** 
The full Audit Log displays.

Chapter 3

Accessing Appliances

Contents

- [Managing appliances](#) on page 39

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

For more information, see:

- [Managing appliances](#)
- [Registering an appliance](#)
- [Editing appliance details](#)
- [Configuring an existing appliance for single sign-on](#)

Related concepts

[Managing appliances](#) on page 39

Related tasks

[Registering an appliance](#) on page 40

[Editing appliance details](#) on page 41

[Configuring an existing appliance for single sign-on](#) on page 42

Managing appliances

Use the page **Appliances > Manage Appliances** to review the Forcepoint appliances registered (associated) with this Security 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
- Version of Forcepoint software (for example, 8.5.4)
- Hardware platform (for example, V5000 G3, V10000 G4, or VMwareOVA)
- Description (can be changed in the CLI with the command "set system host")
- Status of Single Sign-On (enabled/disabled)

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



Important

Single sign-on is supported when the deployment includes the Security Appliance Manager.

The Security Appliance Manager, which replaces the V-Series Appliance Manager, provides a centralized, graphical management console for all Forcepoint appliances in the deployment.

When you register Forcepoint appliances in the Security Manager, you can configure single sign-on. When you click the Single Sign-On button, a page displays that describes how to manage your appliance using the CLI, and provides access to the Content Gateway Manager if Content Gateway is running on the appliance.

- To register an appliance with the Security Manager, see *Registering an appliance*.
- 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*.
- 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.

Related tasks

[Registering an appliance on page 40](#)

[Configuring an existing appliance for single sign-on on page 42](#)

Registering an appliance



Important

Single sign-on is supported when the deployment includes the Security Appliance Manager.

When you register Forcepoint appliances in the Security Manager, you can configure single sign-on. When you click the Single Sign-On button, a page displays that describes how to manage your appliance using the CLI, and provides access to the Content Gateway Manager if Content Gateway is running on the appliance.

To register a new appliance with the Security Manager:

- 1) Click **Register Appliance**.
The Register Appliance window displays.
- 2) In the field **IP address**, enter the IP address for network interface C on the appliance.
- 3) To configure single sign-on from this Security Manager to the appliance, mark the check box **Enable single sign-on from the Security Manager**.
- 4) Enter the administrator password for the appliance.
- 5) To specify Security Manager administrators who have single sign-on permissions for this appliance, click **User Permissions** to expand the User Permissions section.

- 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 grayed out in the **Users with access** list because they have single sign-on access by default, and this cannot be changed.

- 7) Click **OK**.
If configuration is successful, an Appliance Details popup appears confirming the appliance has been added to the Security Manager, and displaying information retrieved from the appliance.

An appliance can only be configured for single sign-on from one Security Manager instance. If another Security Manager 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 the Security Manager, or select **Register without Single Sign-On** to register the appliance and preserve single sign-on configuration on the other Security Manager.

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

If the Security Manager cannot connect to the IP address that you enter, verify the following:

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

To refresh the information for an appliance:

- 1) Click the arrow next to the current appliance IP address to expand the appliance information, and click **Refresh Details**.
- 2) To refresh all of the appliance information on this page, click **Refresh All Appliances**.

To remove an appliance from the list:

- 1) Click the arrow next to the current appliance IP address to expand the appliance information, and click **Unregister**.
A confirmation page displays.
- 2) Click **Yes** to confirm.
The appliance is removed.

Editing appliance details



Important

Single sign-on is supported when the deployment includes the Security Appliance Manager.

When you register Forcepoint appliances in the Security Manager, you can configure single sign-on. When you click the Single Sign-On button, a page displays that describes how to manage your appliance using the CLI, and provides access to the Content Gateway Manager if Content Gateway is running on the appliance.

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 **Edit** 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 the Security Manager cannot connect to the IP address that you enter, verify the following:

- The IP address you entered is the correct one for the appliance's C interface.
- The appliance and Security Appliance Manager are both running.
- The system clock on the Security Manager machine matches the clock on the appliance to within one 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 grayed out in the **Users with access** list because they have single sign-on access by default, and this cannot be changed.

- 5) Click **Save**.
The settings are saved.

Configuring an existing appliance for single sign-on



Important

Single sign-on is supported when the deployment includes the Security Appliance Manager.

When you register Forcepoint appliances in the Security Manager, you can configure single sign-on. When you click the Single Sign-On button, a page displays that describes how to manage your appliance using the CLI, and provides access to the Content Gateway Manager if Content Gateway is running on the appliance.

- 1) From Registered Appliances, click **Configure single sign-on** for the appliance you want to edit.

The Configure Appliance Single Sign-on page displays.

- 2) Mark the check box **Enable single sign-on from the Security Manager**.
- 3) Enter the administrator password for the appliance.
- 4) To specify Security Manager 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 grayed out in the Users with access list, because they have single sign-on access by default, and this cannot be changed.

- 6) Click **OK**.
The settings are saved.

An appliance can only be configured for single sign-on from one Security Manager instance. If another Security Manager 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 Security Manager instance, or select **Register without Single Sign-On** to register the appliance and preserve single sign-on configuration on the other Security Manager.

Chapter 4

Backup and Restore of Global Settings Data

Contents

- [Scheduling management infrastructure backups](#) on page 46
- [Running immediate backups](#) on page 47
- [Restoring management infrastructure backup data](#) on page 48
- [Changing backup settings](#) on page 49

Security Manager settings and system data on the Forcepoint management server machine can be backed up and reverted 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 Forcepoint management server machine.



Important

Make sure that all administrators log off of the Security Manager before you back up or restore a configuration.

The backup process saves:

- Global configuration and infrastructure information, including administrator and appliance data, stored in the Settings Database.
- Certificate files required for the Security Manager browser components. The backup process works as follows:

The backup process works as follows:

- 1) Initiate an immediate backup (see *Running immediate backups*) or define a backup schedule (see *Scheduling management infrastructure backups*).
 - 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*.
- 2) The backup process checks all Forcepoint Management 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 the following:

- EIP.db is a standard PostgreSQL backup file.
- httpd-data.txt contains embedded certificate information and encryption keys.
- backup.txt is created if the backup completes successfully.

- DataBackup.log is 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 Forcepoint security product has its own backup and restore process for the module system settings. See the [Backup and Restore FAQ](#) for comprehensive instructions for all products and modules.

Run Forcepoint Management Infrastructure backups in synchronization with Forcepoint Web Security backups, as described in the FAQ cited above.

Related tasks

[Running immediate backups](#) on page 47

[Scheduling management infrastructure backups](#) on page 46

[Changing backup settings](#) on page 49

Scheduling management infrastructure backups

Before you begin

During management server installation, a scheduled task for backups was created. This task is disabled by default.

Notify Security Manager administrators of the backup schedule, so that they can be sure to log off of the Security 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 is not under significant load.

To schedule backups on Windows Server 2008:

Steps

- 1) On the Forcepoint management server, open the Windows **Task Scheduler**.
- 2) In the Task Scheduler window, select **Task Scheduler Library**.

- 3) Right-click the **Websense TRITON Backup** task and select **Enable**.
- 4) Right-click **Websense 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 Forcepoint management server machine to confirm the changes to the task.

Running immediate backups

Before you begin

Before running a manual backup, make sure that all administrators are logged off of the Security Manager.

To launch an immediate backup:

Steps

- 1) On the Forcepoint management server, open the Windows **Task Scheduler**.
- 2) In the Task Scheduler window, select **Task Scheduler Library**.
- 3) If the **Websense TRITON Backup** task is disabled, right-click the task and select **Enable**.
- 4) Right-click the **Websense TRITON Backup** task and select **Run**.

Restoring management infrastructure backup data

Before you begin

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

Before starting the restore process, it is recommended that you stop the Security Manager services.

To restore Forcepoint Management Infrastructure data:

Steps

- 1) On the Forcepoint management server, open the Windows **Services** tool.
- 2) Right-click the **Websense TRITON Unified Security Center** service and select **Stop**.
- 3) Open the Windows Control Panel and select **Programs > Programs and Features**.
- 4) Select **Forcepoint Management Infrastructure**.
- 5) Click **Uninstall/Change**.
- 6) When asked if you want to add, remove, or modify the Forcepoint Management 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 Unified Security Center” service has not restarted, right-click it and select **Start**

Next steps

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

Before you begin

When the first infrastructure backup is run, 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:

Steps

- 1) On the Forcepoint management server, navigate to the directory **C:\Program Files (X86)\Websense\EIP Infra**.
- 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 (the backup process will not create it), and can be a local or remote path. 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 be accessed by other users. Instead, 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 manually in any previously defined locations.

- 5) Save and close the file. Changes take effect when the next backup is run.

