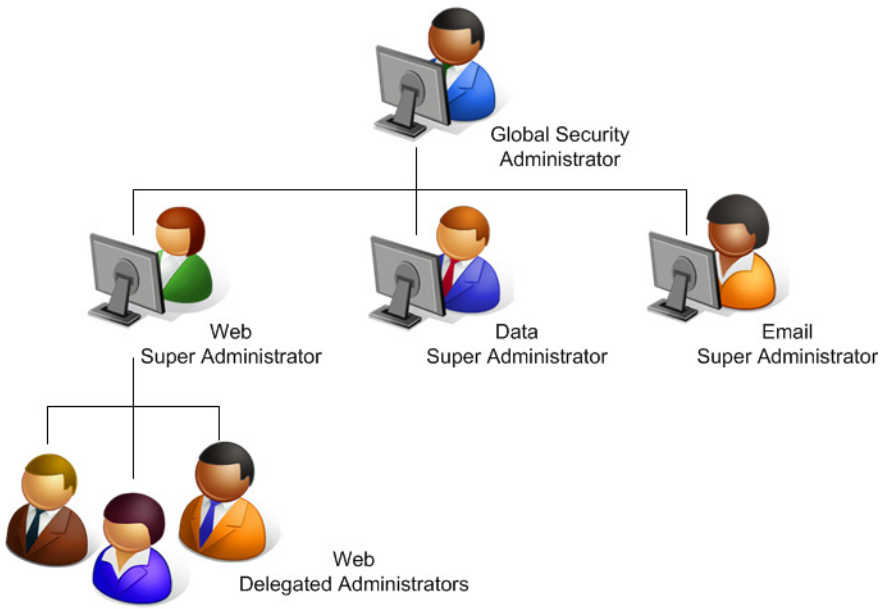
Delegated Administration Quick Start

Delegated Administration | Web Protection Solutions | v8.4.x, v8.5.x | 29-Apr-2022

Delegated administration is a powerful tool for distributing configuration, policy management, and reporting responsibilities across an organization.

Global Security Administrators can define administrator accounts for all Forcepoint Security Manager modules (Web, Data, and Email).

In the Web module, **Super Administrators** can then grant policy management privileges, reporting rights, or both to **delegated administrators**, who can manage or report on Internet usage for specific clients (users, groups, computers, or networks).



Super Administrators can also:

- Create a set of master restrictions that limit the access delegated administrators can grant to their clients via policies.
- Send copies of their policies and filters to delegated administrators, who can use them as templates for creating policies and filters to apply to their clients.

All of this is accomplished through the use of **roles**, which group related clients with the administrators responsible for managing their policies, reporting on their Internet

© 2022 Forcepoint

usage, or both. For example, a school district might create Staff, Teachers, and Elementary Students roles, and then assign one or more administrators to each.

To start using delegated administration, first use the Web module of the Forcepoint Security Manager to prepare your environment:

1. (Optional) *Configure user directory service settings*: Make sure that your web protection software can communicate with a user directory so that you can identify user, group, and domain (OU) clients for use in applying policies.
2. *Customize Super Administrator policies and filters*: Establish a policy baseline for your organization.
3. *Edit the Filter Lock*: Create basic category and protocol management restrictions that apply to all delegated administrators.

When the environment is ready, set up administrator accounts via Global Settings:

1. (Optional) *Configure directory service settings for administrators*: Make sure that the Security Manager can communicate with the directory service used to authenticate administrator logons.
2. *Configure email settings for administrators*: Enable administrator notifications and automated password reset functionality.
3. *Create administrator accounts*: Grant administrators access to the Web module.

Next, use the Web module of the Forcepoint Security Manager to enable delegated administration of policy management and reporting tasks.

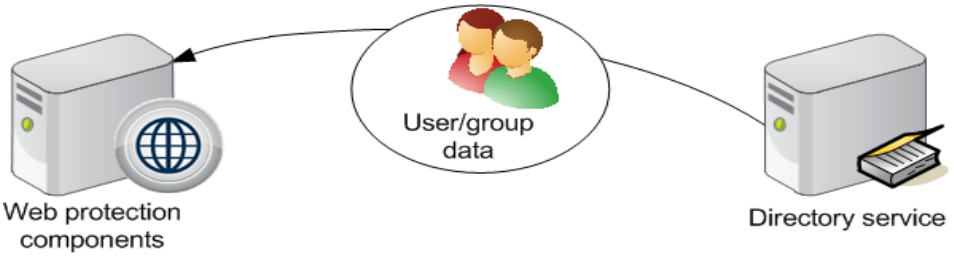
1. *Create Web delegated administration roles*: Define which administrators will manage policies, run reports, or both for which groups of clients.
2. *Train delegated administrators*: Make sure that new administrators know how to perform their tasks.

This Quick Start guide provides the basic information needed to get started with delegated administration. Complete and comprehensive instructions are available from the Administrator Help, available from the Help menu in the Security Manager, or from the Technical Library.

Configure user directory service settings

Delegated Administration | Web Protection Solutions | v8.4.x, v8.5.x | 29-Apr-2022

In order for your web protection software to manage and report on Internet usage for users, groups, and domains (OUs) defined in your directory service, User Service must be installed and configured to communicate with the directory.



If your organization assigns policies exclusively based on IP addresses, you can skip this section.

Windows Active Directory (native mode), Novell eDirectory, and Oracle (formerly Sun Java) Directory Server are all supported.

To configure directory service settings in the Web module of the Forcepoint Security Manager:

1. Click the **Settings** option in the left navigation pane, and then select **Directory Services**.
2. Select a directory from the **Directories** list.

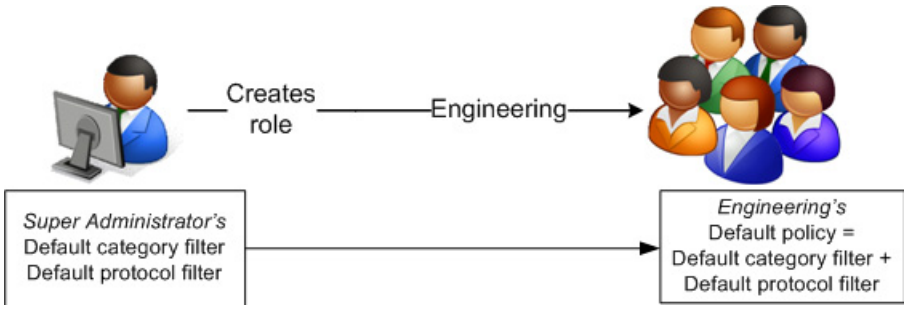
   Provide configuration information as prompted. See the “Directory Services” topic in Administrator Help for detailed instructions.

Customize Super Administrator policies and filters

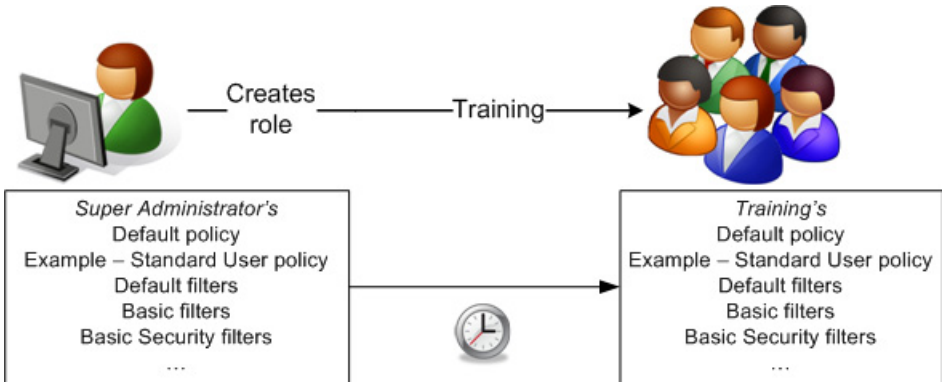
Delegated Administration | Web Protection Solutions | v8.4.x, v8.5.x | 29-Apr-2022

When you create each delegated administration role, you can select how policies and filters are created for the new role:

- By default, only the current Default category and protocol filters in the Super Administrator role are automatically copied to each new role, and a Default policy that enforces those filters is created.



- Alternatively, you can copy all policies, filters, custom categories, custom URLs, and keywords from the Super Administrator role to the new delegated administration role at the time of creation. This may take a long time (15 minutes or more) if there are many policies, filters, and filter components in the Super Administrator role.



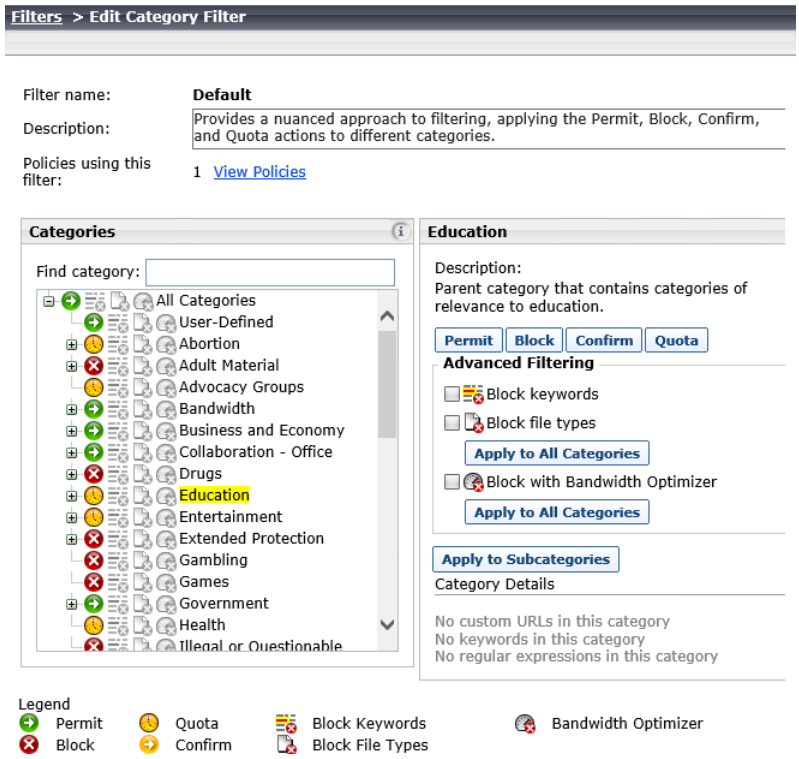
  - If you are logged out of the Security Manager while information is being copied to a role, the copy process will continue on its own. You may not be able to log back on to the Security Manager, however, until the copy process is complete.
  - The special Permit All category and protocol filters are not subject to the Filter Lock, and cannot be used in delegated administration roles. When you copy a policy that uses a Permit All filter to a delegated administration role, a new filter (Permit Categories [Modified] or Permit Protocols [Modified]) is created in the role that permits all categories and protocols not blocked and locked by the Filter Lock. See *Edit the Filter Lock*.

Changes made to the filters and policies in the Super Administrator role are not automatically reflected in the policies and filters in other roles. After delegated administration roles have been created, however, any Super Administrator can:

- Use the **Copy to Role** option to push changes to policies and filters to delegated administration roles.
- Copy additional policies and filters to delegated administration roles.

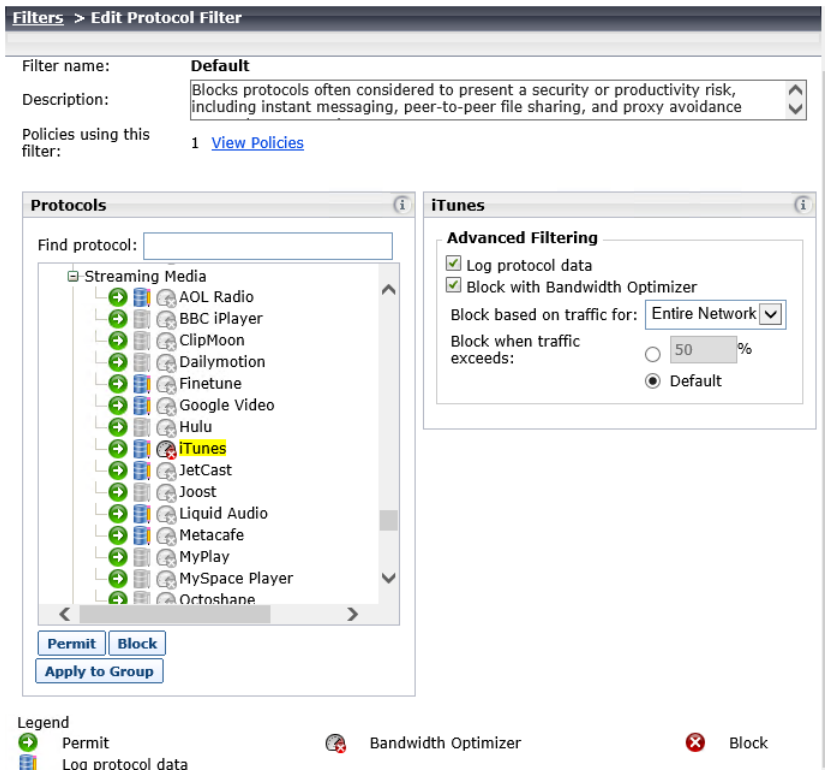
As a best practice, in order to ensure that the Super Administrator policies and filters provide a useful baseline for delegated administrators, Super Administrators should review at least the Default filters before creating roles.

1. In the Web module of the Forcepoint Security Manager, select **Main > Policy Management > Filters** from the left navigation pane.
2. In the Category Filters list, click **Default**.



3. Scroll through the Categories list to ensure that the appropriate action is applied to each parent category and subcategory.
   - To change the action applied to a category, select the category, and then use the buttons at the bottom of the list.
   - You can also use the Advanced Filtering check boxes to the right of the Categories list to change keyword blocking, file type blocking, and Bandwidth Optimizer settings.
4. If you have made any changes, click **OK** to cache them and return to the Filters page. Changes are not implemented until you click **Save All** or **Save and Deploy**.

5. In the Protocol Filters list, click **Default**.



6. Scroll through the Protocols list to ensure that the appropriate action is applied to each protocol.
   - To change the action applied to a protocol, use the buttons at the bottom of the list.
   - You can also use the Advanced Filtering check boxes to the right of the Protocols list to change logging or Bandwidth Optimizer settings.
7. If you have made any changes, click **OK** to cache them and return to the Filters page. Changes are not implemented until you click **Save All** or **Save and Deploy**.

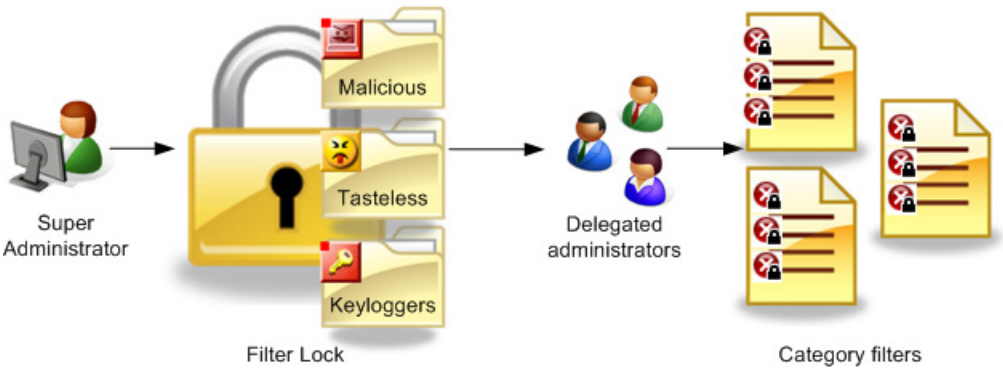
Remember that although the Super Administrator policies and filters should be a useful guideline for delegated administrators, those administrators can edit the policies and filters within their roles, and create new policies and filters.

Edit the Filter Lock

Delegated Administration | Web Protection Solutions | v8.4.x, v8.5.x | 29-Apr-202229-Apr-2022

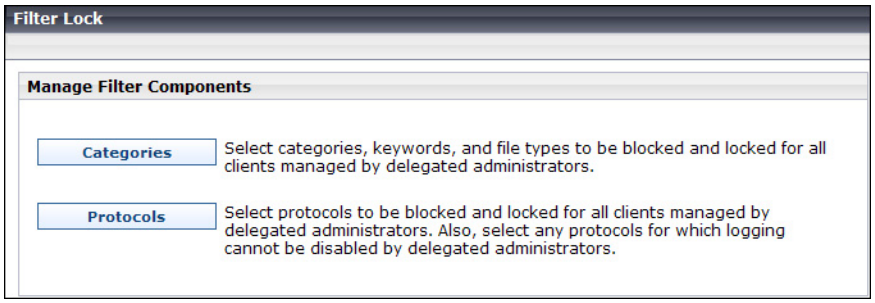
Unconditional Super Administrators can create a Filter Lock to define categories and protocols that delegated administrators cannot permit for any clients. When delegated administrators edit policies, categories and protocols that a Super Administrator has

blocked via the Filter Lock appear **Blocked and Locked** (the red Block icon is displayed with an overlapping Lock icon).

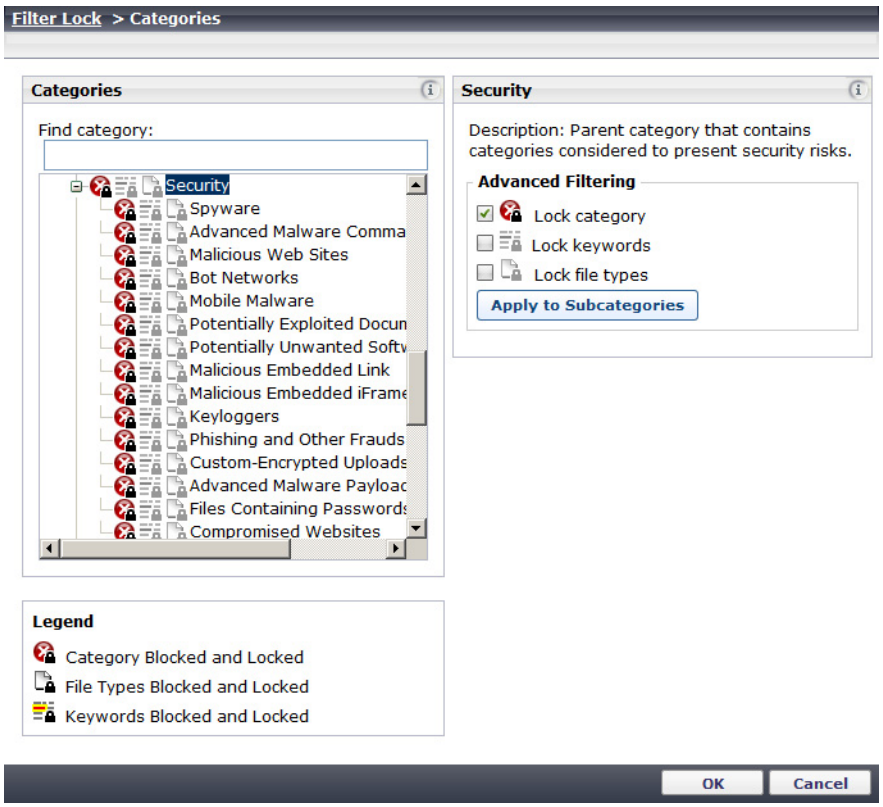


Clients managed by the Super Administrator role can be given access to categories and protocols blocked and locked for clients managed in other roles. For example, if company executives, members of the legal team, or investigators were managed by the Super Administrator role, they can be given access to sites blocked for most members of the organization.

1. Select **Main > Policy Management > Filter Lock** from the left navigation pane.



2. Under Manage Filter Components, click **Categories**.



3. Scroll to the first category that you want to lock, and then click the category name. Expand parent categories to see subcategories.
4. Use the Advanced Filtering check boxes to select which features you want to lock for the selected category:
   - **Lock category** blocks access to the category.
   - **Lock keywords** causes keyword blocking to be enabled.
   - **Lock file types** causes file-type blocking to be enabled.

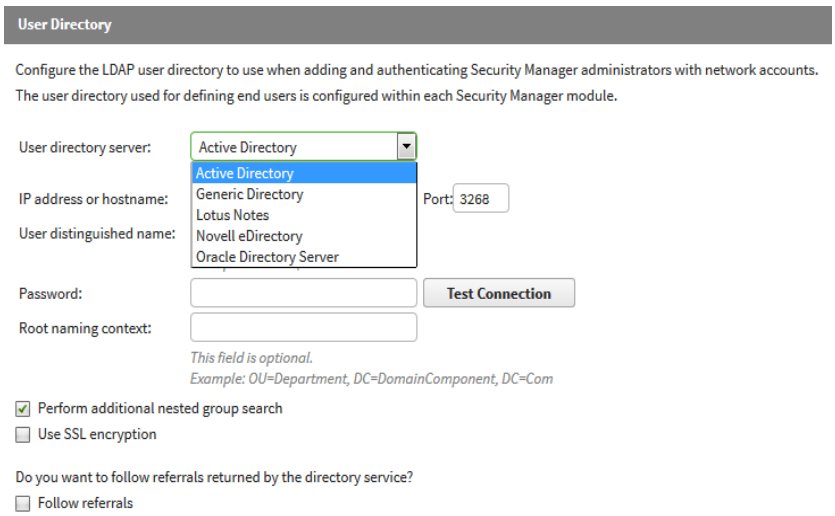
   These settings affect all category filters managed by delegated administrators in all roles (**except** for those managed by the Super Administrator role).
5. Repeat for each additional category that you want to lock.
6. When you are finished making changes, click **OK** to return to the Filter Lock page.
7. Under the Manage Filter Components, click **Protocols**.
8. As with categories, identify the protocols that you want to block and lock, and use the Advanced Filtering check boxes to make your changes.
9. When you are finished, click **OK** to return to the Filter Lock page.
10. Click **Save All** or **Save and Deploy** to implement your changes to the Filter Lock.

Configure directory service settings for administrators

Administrative users can log on to the Security Manager using either local accounts or their network accounts. In order to enable administrators to use their network logons, you must configure the Security Manager to communicate with a single directory server to authenticate those logons.

If you prefer that administrators use only local accounts to log on to the Security Manager, you can skip this section.

1. Go to the **Global Settings > User Directory** page in the Security Manager.



2. Select your directory service type from the **User directory server** list.

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

   - Windows Active Directory
   - Generic Directory (LDAP directory service not otherwise listed)
   - Lotus Notes
   - Novell eDirectory
   - Oracle Directory Server (formerly Sun Java Directory)

3. Provide configuration information as prompted. Go to **Help > Explain This Page** on the User Directory page for detailed instructions for configuring directory communication for administrator authentication.

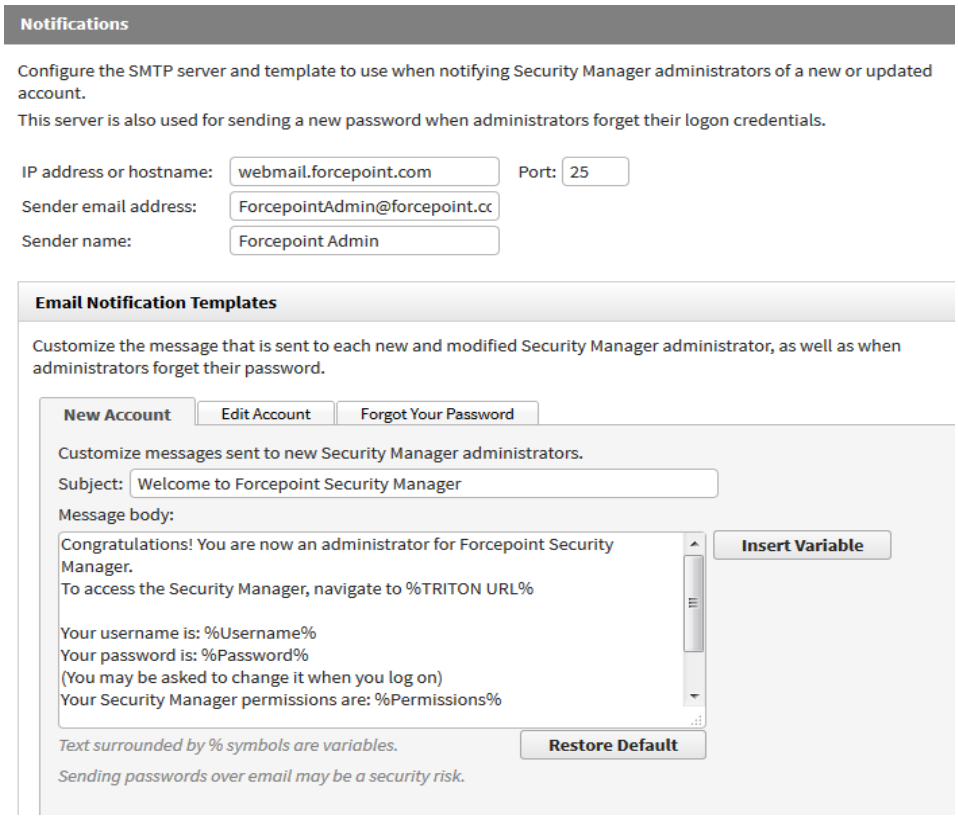
Configure email settings for administrators

Each administrator account configured on the Global Settings page is required to have an associated email address. The email address is used to optionally notify administrators that they have been given administrative access to one or more modules of the Security Manager. It is also used for password recovery.

To enable email notifications and password recovery, provide SMTP information in the Security Manager. If you performed this step during installation, you do not need to repeat the configuration.

To configure SMTP settings:

1. Go to the **Global Settings > Notifications** page in the Security Manager.



2. Enter the **IP address or host name** and the **Port** of a valid SMTP server in your network.
3. Enter the **Sender email address** that will appear in notifications.
4. Optionally, 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 Security Manager.
5. Review the templates used for administrator notifications. There are 3 available:

- **New Account** notifies administrators of their new administrator account. By default, this includes the new logon name and password, and a summary of the permissions allocated to the administrator.
- **Edit Account** notifies administrators of any changes to their Security Manager account, such as a password or permissions change.
- **Forgot Your Password** confirms to administrators using the password recovery feature that their password has been reset. By default, this includes a temporary password and password expiration details.

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%**.

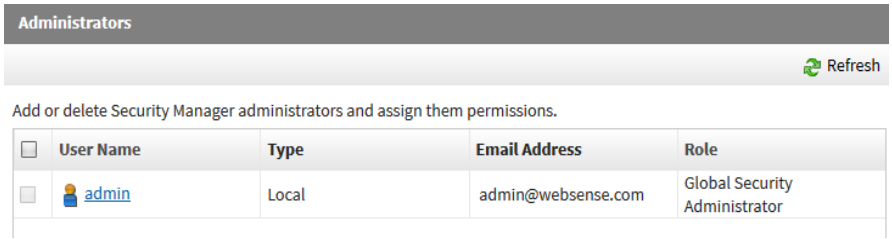
Create administrator accounts

Delegated Administration | Web Protection Solutions | v8.4.x, v8.5.x | 29-Apr-2022

Administrator accounts for all Forcepoint Security modules are centrally created and maintained on the **Global Settings > Administrators** page. Global Security Administrators add accounts and grant them permission to access one or more Forcepoint Security modules. Accounts cannot be added to delegated administration roles until they have first been created in Global Settings.

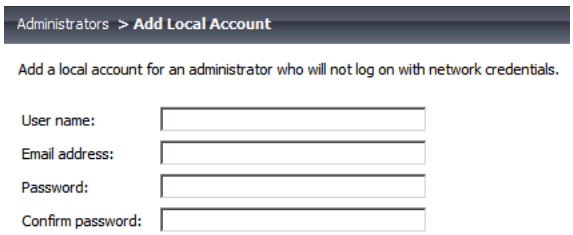
To define administrator accounts with access to the Web module of the Forcepoint Security Manager:

1. Go to the **Global Settings > Administrators** page. Initially, only the **admin** account is listed on this page.

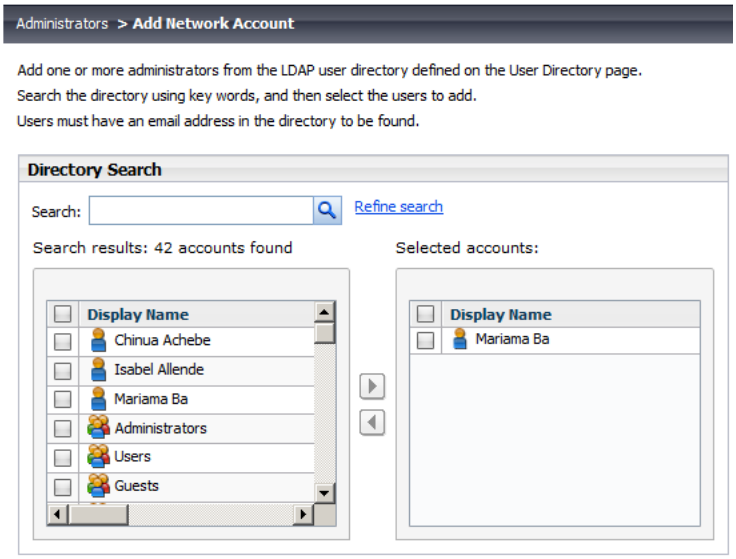


2. Click **Add Local Account** or **Add Network Account** to define an administrator account.
   - A local account is used only to access the Security Manager. You define the account name and password, and manually associate an email address with the account.
   - A network account is a user or group account defined in the directory service configured on the **Global Settings > User Directory** page. In order to be defined as an administrator, the user or group account must have an email attribute assigned.
3. Do one of the following:

- Enter a **User name**, **Email address**, and **Password** for the local account.

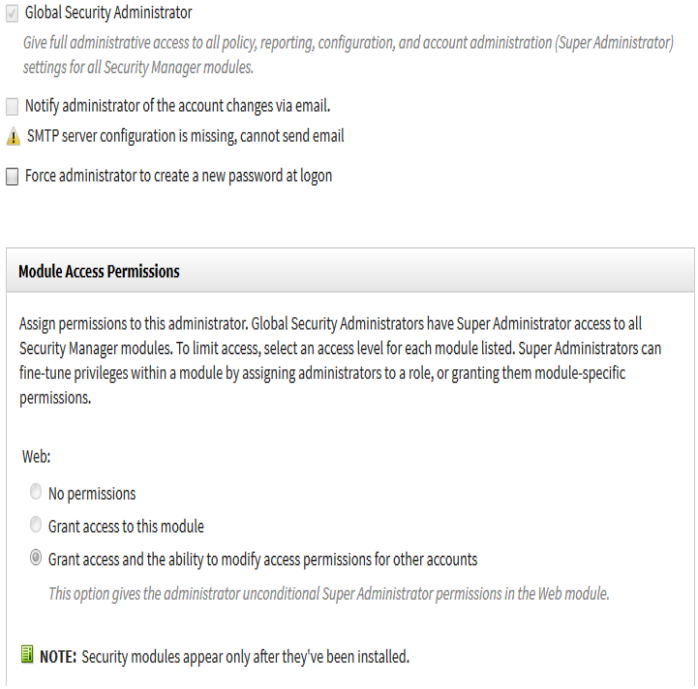


- Enter all or part of a user or group name in the **Search** box, then select one or more users or groups to add to the **Selected accounts** list.



4. Specify whether or not to **Notify administrator of the new account via email**. You can customize the email message sent to new administrators on the **Global Settings > Notifications** page.
5. If you are adding a local account, specify whether or not to **Force administrator to create new password at logon**. Local administrators can change their own password at any time on the **Global Settings > My Account** page.

6. Define the general level of Web module management access for this account.



   - Select **Grant access to this module** to provide only basic Web module access. Until the account is assigned to a role and granted delegated administrator permissions within the Web module, it can be used only to access a limited subset of the **Status > Dashboard** page.
   - Select **Grant access and the ability to modify access permissions for other accounts** to define the account as an unconditional Super Administrator. Once you click OK, the new administrator is given full access to all Web module features and functions.
7. Click **OK** to save your changes and create the account. The account is immediately available for configuration within the Web module.
8. Repeat to create additional administrators, as needed.

Create Web delegated administration roles

Delegated Administration | Web Protection Solutions | v8.4.x, v8.5.x | 29-Apr-2022

Delegated administration roles are made up of any number of related clients (directory, computer, or network) and the administrators who manage their policies, run reports on their Internet usage, or both. There are 2 role types:

- **Policy management and reporting**: User policies are managed by administrators in the role. Administrators in the role can optionally also run reports, either on clients in the role, or on all clients.

  Clients can be added to only one policy management and reporting role.

- **Investigative reporting**: Administrators can run investigative reports showing Internet activity for only managed clients in the role. Client policies are managed in other roles.

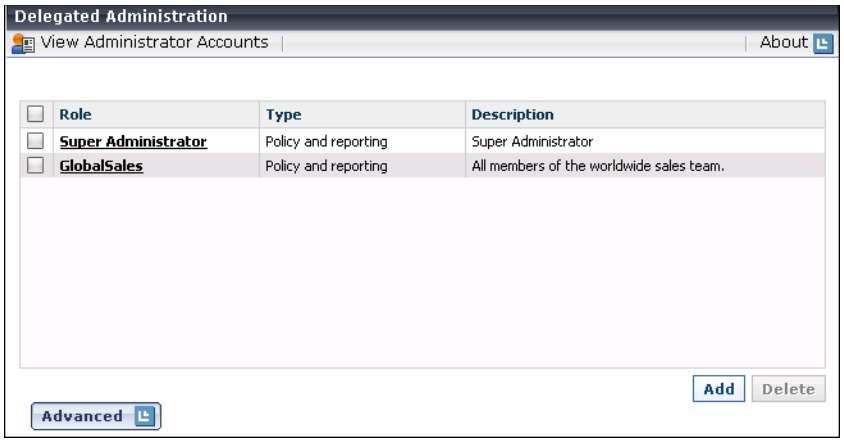
  Clients can be added to multiple investigative reporting roles.

A role can include multiple administrators, and different administrators within a role can have different privileges. For example, the Intern policy management and reporting role might have one administrator responsible for creating policies, but who does not have any reporting permissions, and another administrator responsible for running weekly or monthly reports on Internet usage by clients in the role, but with no policy permissions.

Super Administrators manage policy for those clients not assigned to a delegated administration role.

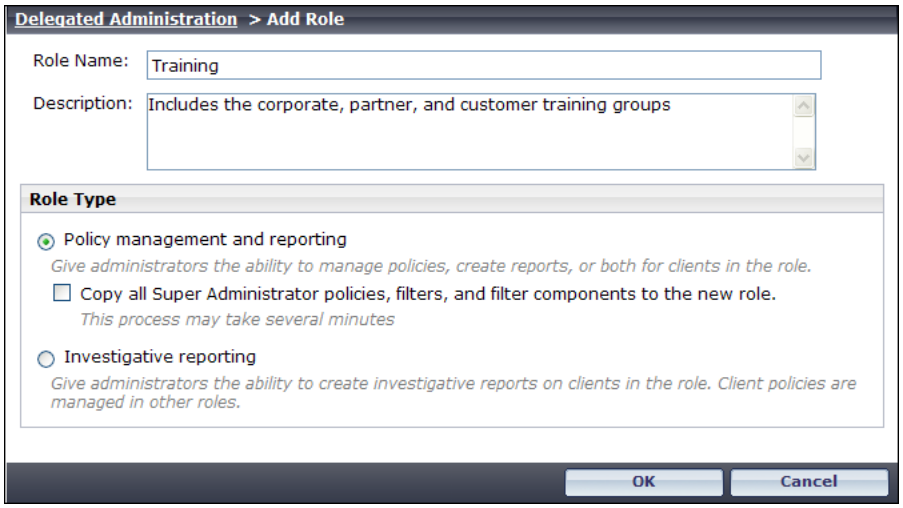
To create a role:

1. In the Security Manager, go to the **Main > Policy Management > Delegated Administration** page. A list of existing roles is displayed. Initially, this shows only the Super Administrator role.

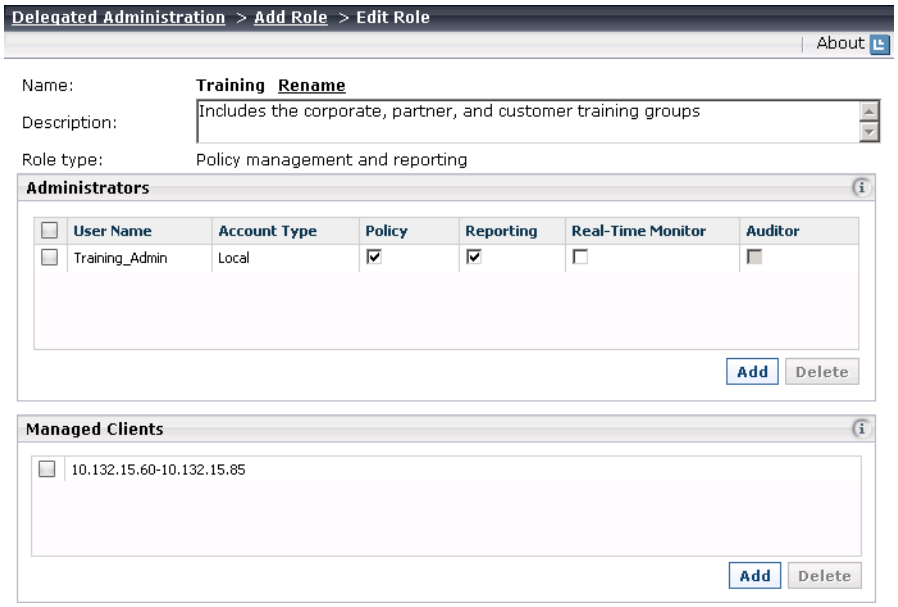


2. Click **Add**.
3. Provide a **Role Name** and **Description**, and then specify the role type.
   - The role type determines the permissions that can be granted to administrators in the role.
   - If you are creating a **policy management and reporting role**, indicate whether to copy all Super Administrator policies, filters, and filter components to the new role.

If this option is not selected, only one policy is created for the role: a Default policy that enforces a copy of the Super Administrator's Default category and protocol filters.



4. Click **OK** to continue to the Edit Role page, where you can define the administrators and clients in the role.



Add administrators to the role

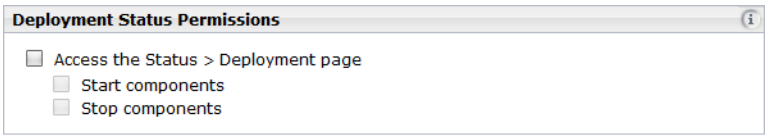
To add delegated administrators:

1. Click the **Add** button below the Administrators list.
2. Select administrators to add to the role, and then click the appropriate right-arrow button to add them to the Selected list.

3. If you have created a *policy management and reporting* role, use the **Policy management**, **Reporting**, and **Real-Time Monitor** check boxes to indicate which general permissions the selected administrators should have. If you grant policy permissions, also select a radio button:
   - **Full policy** permissions allow administrators to create and manage policies, filters, filter components, and exceptions for their managed clients.
   - **Exceptions only** permissions allow administrators to create exceptions that permit or block specific URLs for managed clients, but not to create or edit policies, filters, or filter components.
   - **Auditor** permissions allow administrators *read-only* access to the policy management features accessible to administrators with full policy permissions in the role.

   If you have created an *investigative reporting* role, there are no permissions to configure on this page.
4. Click **OK** to return to the Edit Role page.
5. Refine permissions for administrators in the role as follows:
   - For *policy management and reporting* roles, optionally update the permissions granted to an administrator using the **Policy Management** drop-down list and the **Reporting** and **Real-Time Monitor** check boxes in the Administrators list.

     Under **Deployment Status Permissions**, specify whether administrators can view the Status > Deployment page, and whether they can use the page to start and stop components.

     Under **Reporting Permissions**, specify which reporting tools administrators with reporting permissions can access.
   - For *investigative reporting* roles, use the **Reporting Permissions** check boxes to determine what reporting features are available to administrators in the role. Options that require permissions to report on all clients are disabled.

When you are finished adding administrators, continue with *Add clients to the role*, page 16.

Add clients to the role

To add clients to the role:

1. Click the **Add** button under the Managed Clients list to add clients to the role.
2. Select or enter clients to add, and then click the right-arrow button to move them to the Selected list.

- Expand the Directory Entries tree to browse your directory service for users, groups, and domains (OUs). Mark the check box next to an entry to select it.
- Enter individual IP addresses or IP address ranges to add as computer and network clients in this role.

Important

Clients can be added to only **one** *policy management and reporting* role.

- IP addresses and ranges added to one role cannot overlap IP addresses and ranges already added to other roles.
- If a user belongs to 2 groups, each of which is in a separate role, you can configure which role's policy takes precedence. See the Administrator Help for details.

3. Click **OK** to return to the Edit Role page.

When you are finished making changes to the role, click **OK** to return to the Delegated Administration page, and then click **Save All** or **Save and Deploy** to implement your changes.

Train delegated administrators

Delegated Administration | Web Protection Solutions | v8.4.x, v8.5.x | 29-Apr-2022

After creating delegated administration roles, make sure that new administrators understand how to:

1. Access the Security Manager (both the URL, and which logon account to use).
2. Select the appropriate role (for those managing more than one role).
3. Create filters and policies.
4. Add managed clients to their Clients page and assign them a policy.
5. Create exceptions to permit or block individual URLs for specified clients.
6. Access reporting tools to generate and schedule reports.

Detailed instructions for performing common policy and reporting tasks are available in the New Admin Quick Start tutorial and Administrator Help. Both can be accessed from the Help menu in the Security Manager, or from support.forcepoint.com.

The Find Answers box in the shortcut pane on the right also provides links to relevant information.

©2022 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.