

Delegated Administration Quick Start

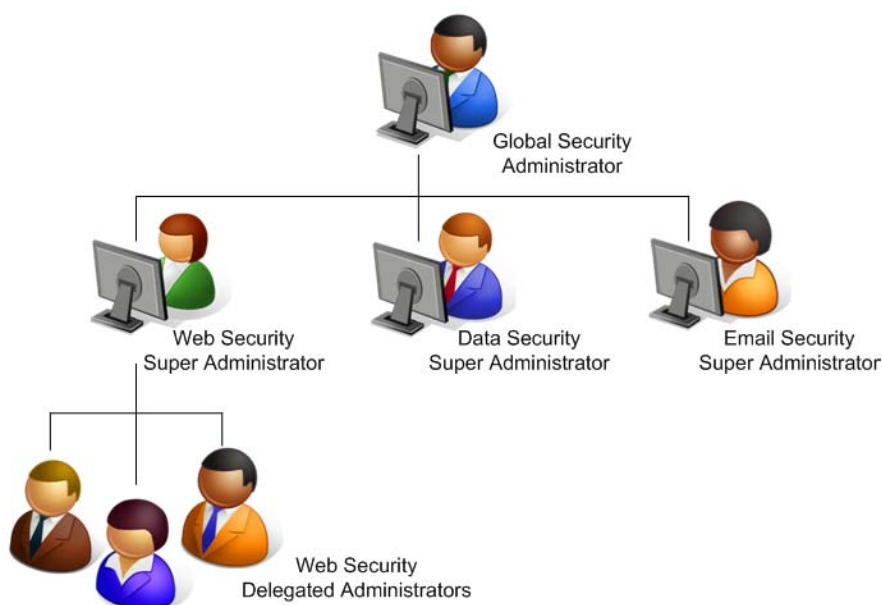
Topic 50200 | Delegated Administration Quick Start | Updated 22-Oct-2013

Applies to: Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6, 7.7, and 7.8

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 TRITON console modules (Web Security, Data Security, and Email Security).

In the Web Security 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 in Web Security 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 Web Security policies, reporting on their Internet 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 Security module of the TRITON console (Web Security manager) to prepare your environment:

1. (Optional) *Configure user directory service settings*: Make sure that your Web Security solution can communicate with a user directory so that you can add user, group, and domain (OU) clients to the Web Security manager.
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 TRITON Settings:

4. (Optional) *Configure directory service settings for administrators*: Make sure that the TRITON Unified Security Center can communicate with the directory service used to authenticate administrator logons.
5. *Configure email settings for administrators*: Enable administrator notifications and automated password reset functionality.
6. *Create administrator accounts*: Grant administrators access to the Web Security module.

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

7. *Create delegated administration roles in the Web Security manager*: Define which administrators will manage policies, run reports, or both for which groups of clients.
8. *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 Web Security Help, available from the Help menu in the Web Security manager, or from the [Websense Technical Library](#).

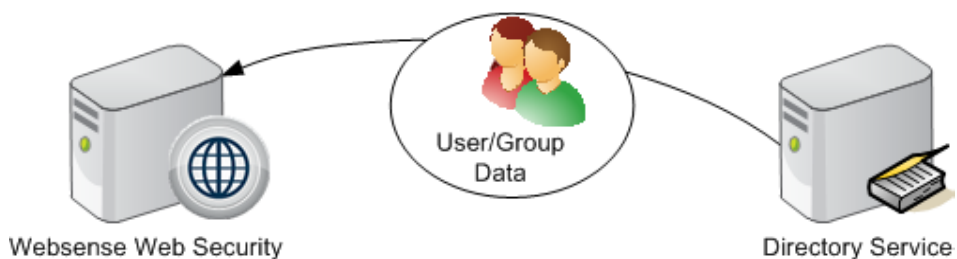
Configure user directory service settings

Topic 50201 | Delegated Administration Quick Start | Updated 22-Oct-2013

Applies to:

Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6, 7.7, and 7.8

In order for Websense Web Security to manage and report on Internet usage for users, groups, and domains (OUs) defined in your directory service, Websense 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.

Websense Web Security can communicate with Windows Active Directory (native or mixed mode), Novell eDirectory, and Oracle (formerly Sun Java) Directory Server.

To configure directory service settings in the Web Security manager:

1. Click the **Settings** tab of the left navigation pane, and then select **Directory Services**.
2. Select a directory from the **Directories** list.
3. Provide configuration information as prompted. Refer to the “Directory Services” section of the Web Security Help ([version 7.6](#), [version 7.7](#), or [version 7.8](#)) for detailed instructions.



Warning

If you initially configure Websense software to communicate with Windows Active Directory in mixed mode, and later change your configuration to use native mode, you must remove existing directory clients from the Web Security manager, and then re-add them.

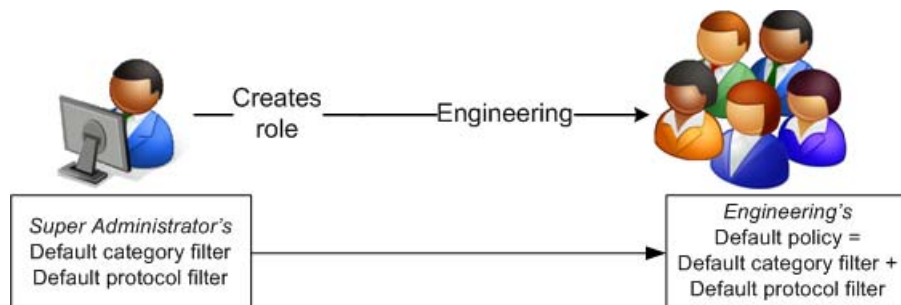
Customize Super Administrator policies and filters

Topic 50202 | Delegated Administration Quick Start | Updated 22-Oct-2013

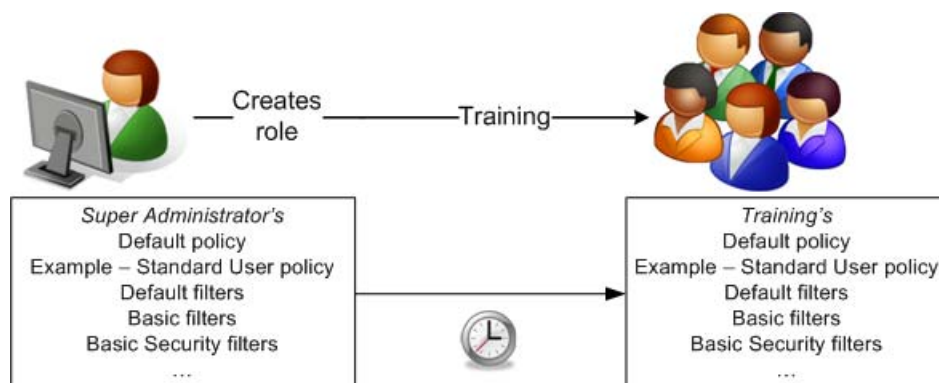
Applies to: Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6, 7.7, 7.8

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 TRITON console 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 TRITON console, however, until the copy process is complete.

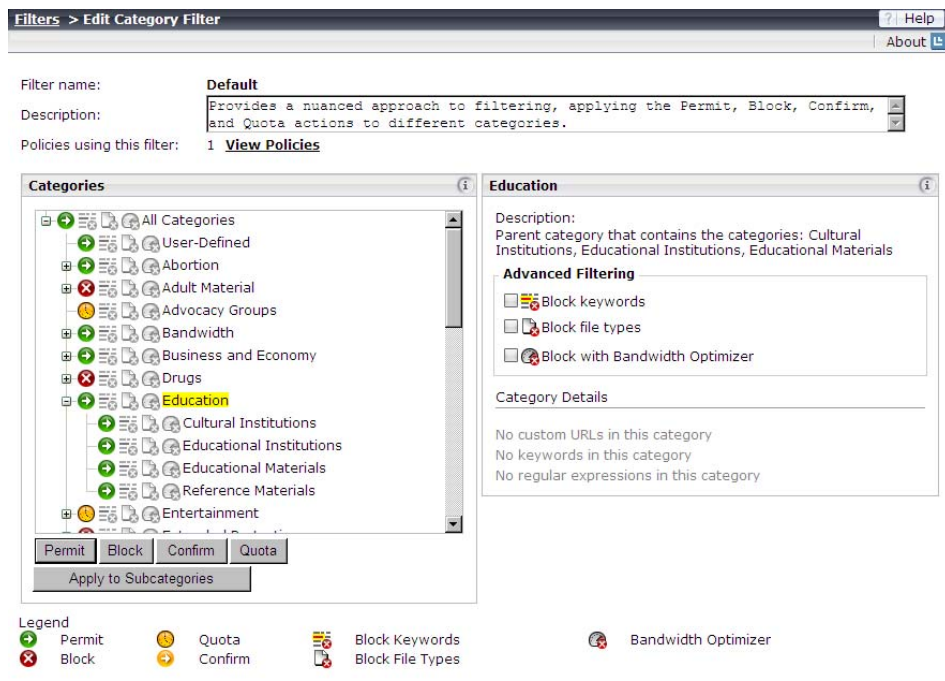
- The special Permit All category and protocol filters are not subject to the Filter Lock, and cannot be used in delegated administration roles. When you copy a policy that uses a Permit All filter to a delegated administration role, a new filter (Permit Categories [Modified] or Permit Protocols [Modified]) 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.

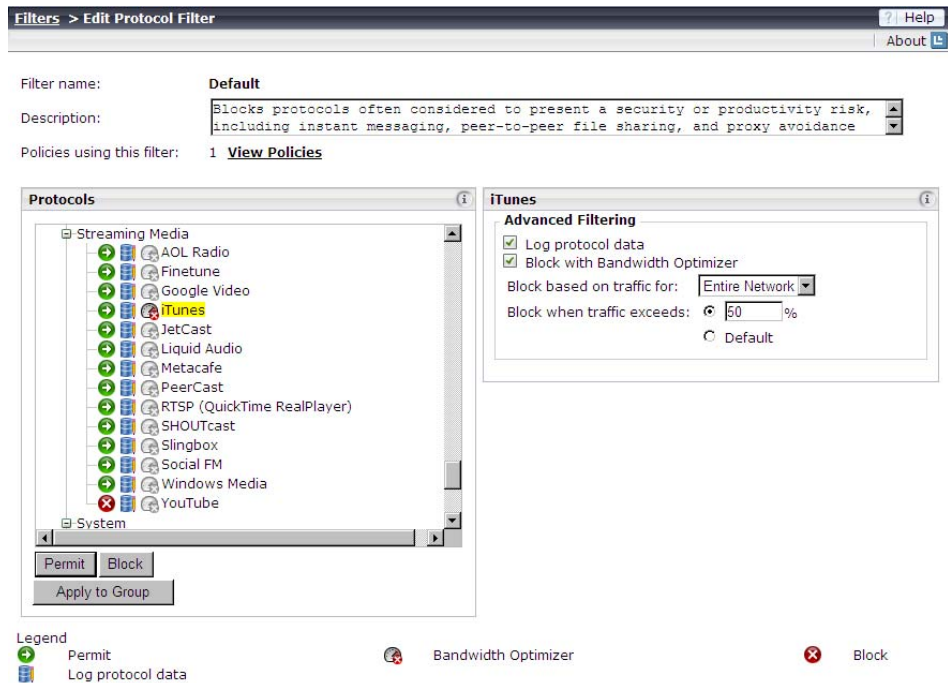
As a best practice, in order to ensure that the Super Administrator policies and filters provide a useful baseline for delegated administrators, Super Administrators should review at least the Default filters before creating roles.

1. In the Web Security manager, on the **Main** tab of the left navigation pane, select **Filters**.
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

Topic 50203 | Delegated Administration Quick Start | Updated 22-Oct-2013

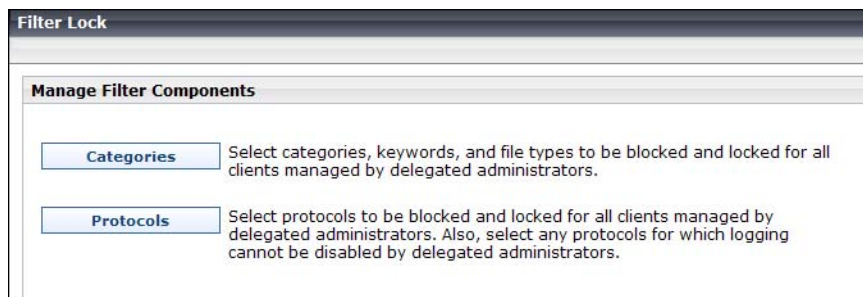
Applies to: Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6, 7.7, and 7.8

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).

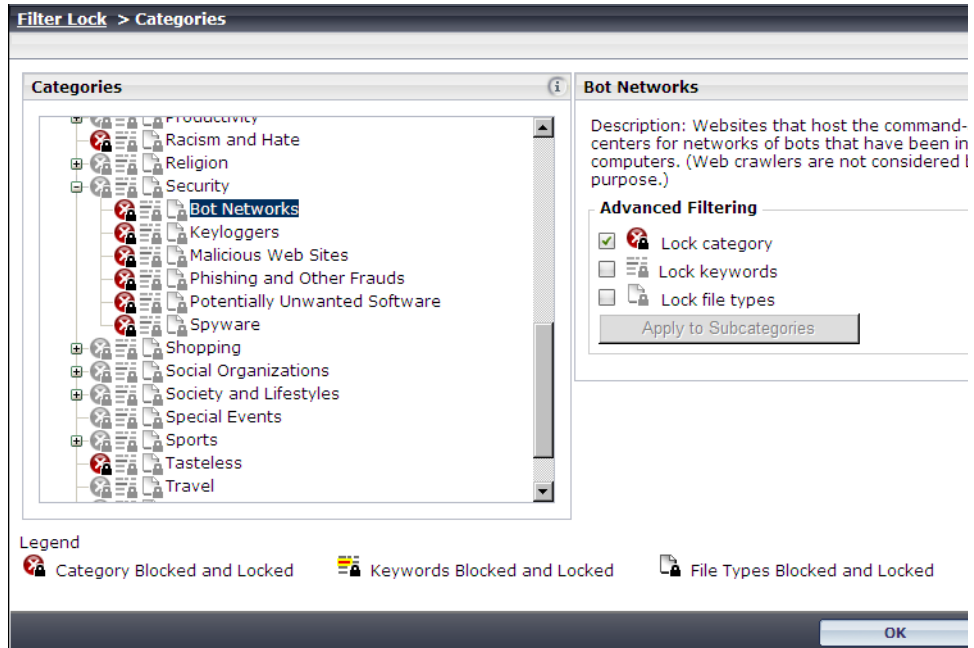


Clients managed by the Super Administrator role can be given access to categories and protocols blocked and locked for clients managed in other roles. For example, if company executives, members of the legal team, or investigators were managed by the Super Administrator role, they can be given access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

1. On the **Main** tab of the left navigation pane, click **Filter Lock** (under Policy Management).



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

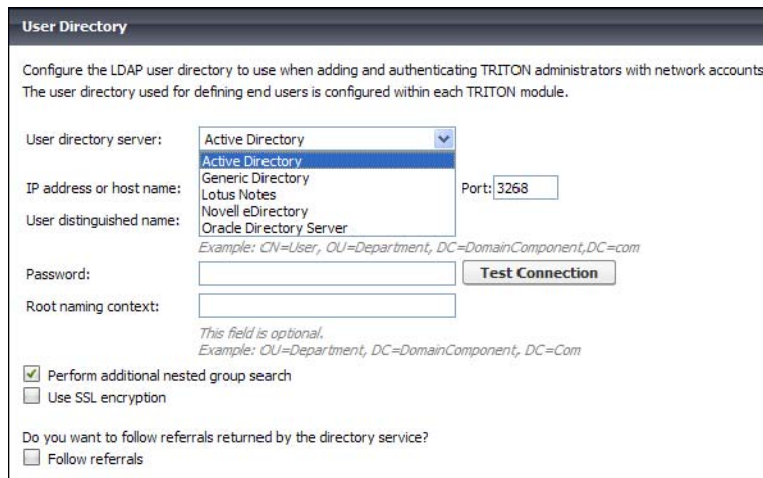
Topic 50204 | Delegated Administration Quick Start | Updated 22-Oct-2013

Applies to: Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6, 7.7, and 7.8

Administrative users can log on to the TRITON console using either local accounts or their network accounts. In order to enable administrators to use their network logons, you must configure the TRITON Unified Security Center 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 TRITON console, you can skip this section.

1. Go to the **TRITON Settings > User Directory** page in the TRITON console.



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

Topic 50205 | Delegated Administration Quick Start | Updated 22-Oct-2013

Applies to: Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6, 7.7, and 7.8

Each administrator account configured in the TRITON Unified Security Center 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 TRITON console. It is also used for password recovery.

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

To configure SMTP settings:

1. Go to the **TRITON Settings > Notifications** page in the TRITON console.

The screenshot shows the 'Notifications' configuration page in the TRITON console. The page is divided into two main sections: 'Notifications' and 'Email Notification Templates'.

Notifications Section:

- Header: Notifications
- Instruction: Configure the SMTP server and template to use when notifying TRITON administrators of a new or updated account. This server is also used for sending a new password when administrators forget their logon credentials.
- Fields: IP address or host name (text input), Port (text input, value: 25), Sender email address (text input), and Sender name (text input).

Email Notification Templates Section:

- Header: Email Notification Templates
- Instruction: Customize the message that is sent to each new and modified TRITON administrator, as well as when administrators forget their password.
- Buttons: New Account, Edit Account, Forgot Your Password
- Section: Customize messages sent to new TRITON administrators.
- Subject: Welcome to Websense TRITON (text input)
- Message body: A text area containing a template message with variables: Congratulations! You are now an administrator for Websense TRITON Unified Security Center. To access Triton, navigate to %TRITON URL%. Your username is: %Username%. Your password is: %Password%. (You may be asked to change it when you log on) Your TRITON permissions are: %Permissions%. Regards, Websense TRITON support.
- Buttons: Insert Variable (dropdown), Restore Default
- Footnote: Text surrounded by % symbols are variables. Sending passwords over email may be a security risk.

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 TRITON console.
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 TRITON 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

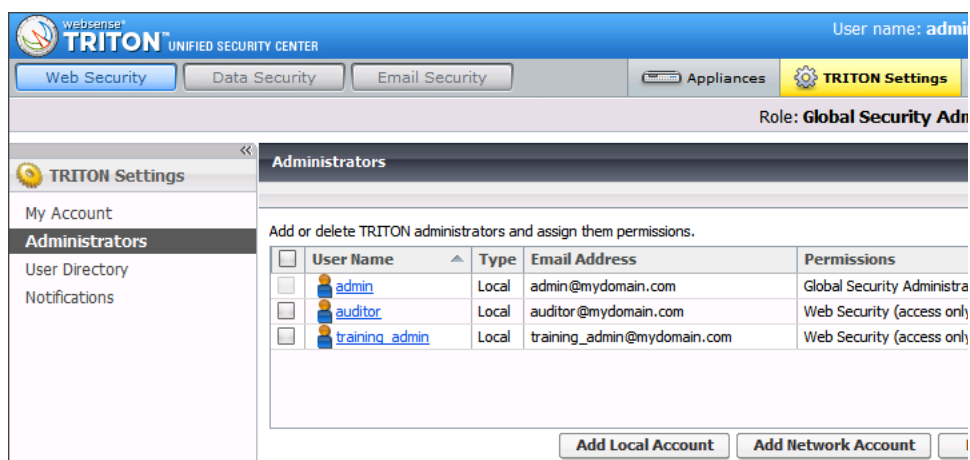
Topic 50206 | Delegated Administration Quick Start | Updated 22-Oct-2013

Applies to: Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6, 7.7, 7.8

Administrator accounts for all TRITON modules are centrally created and maintained on the **TRITON Settings > Administrators** page. Global Security Administrators add accounts and grant them permission to access one or more TRITON modules. Accounts are not available to be configured as Web Security delegated administrators until they have been added in TRITON Settings.

To define administrator accounts with Web Security access:

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



The screenshot shows the TRITON Unified Security Center interface. The top navigation bar includes 'Web Security', 'Data Security', 'Email Security', 'Appliances', and 'TRITON Settings'. The user is logged in as 'admin' with the role 'Global Security Administrator'. The left sidebar shows 'TRITON Settings' with sub-items: 'My Account', 'Administrators', 'User Directory', and 'Notifications'. The main content area is titled 'Administrators' and contains the following table:

<input type="checkbox"/>	User Name	Type	Email Address	Permissions
<input type="checkbox"/>	admin	Local	admin@mydomain.com	Global Security Administrator
<input type="checkbox"/>	auditor	Local	auditor@mydomain.com	Web Security (access only)
<input type="checkbox"/>	training_admin	Local	training_admin@mydomain.com	Web Security (access only)

At the bottom right of the table area, there are two buttons: 'Add Local Account' and 'Add Network Account'.

2. Click **Add Local Account** or **Add Network Account** to define an administrator account.
 - A local account is used only to access the TRITON console. 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 **TRITON 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.

Administrators > Add Local Account

Add a local account for an administrator who will not log on with network credentials.

User name:

Email address:

Password:

Confirm password:

- 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.

Administrators > Add Network Account

Add one or more administrators from the LDAP user directory defined on the User Directory page.
Search the directory using key words, and then select the users to add.
Users must have an email address in the directory to be found.

Directory Search

Search: [Refine search](#)

Search results: none found

<input type="checkbox"/>	Display Name	User Name	Email Address
--------------------------	--------------	-----------	---------------

Show Previous Show Next

Selected accounts: **None**

Adding an item will override the

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 **TRITON 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 **TRITON Settings > My Account** page.

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

Module Access Permissions

Assign permissions to this administrator. Global Security Administrators have Super Administrator access to all TRITON modules. To limit access, select "Custom".

Super Administrators can fine-tune privileges within a module by assigning administrators to a role, or granting administrators module-specific permissions.

Global Security Administrator

Give full administrative access to all policy, reporting, configuration, and account administration (Super Administrator) settings for all TRITON modules.

Custom

Assign this administrator access to one or more modules. Also indicate whether the administrator can manage other administrator accounts within each module.


Web Security:

No permissions

Grant access to this module

Grant access and the ability to modify access permissions for other accounts

This option gives the administrator unconditional Super Administrator permissions in the Web Security module.

 **NOTE:** Security modules appear only after they've been installed.

- Select **Grant access to this module** to provide only basic Web Security access. Until the account is assigned to a role and granted delegated administrator permissions within the Web Security module, it can be used only to access the Web Security Dashboard (v7.7 and later) or Today page (v7.6).
 - 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 Security features and functions.
7. Click **OK** to save your changes and create the account. The account is immediately available for configuration within the Web Security module.
 8. Repeat to create additional administrators, as needed.

Create delegated administration roles in the Web Security manager

Topic 50207 | Delegated Administration Quick Start | Updated 22-Oct-2013

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6, 7.7, and 7.8
--------------------	---

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.

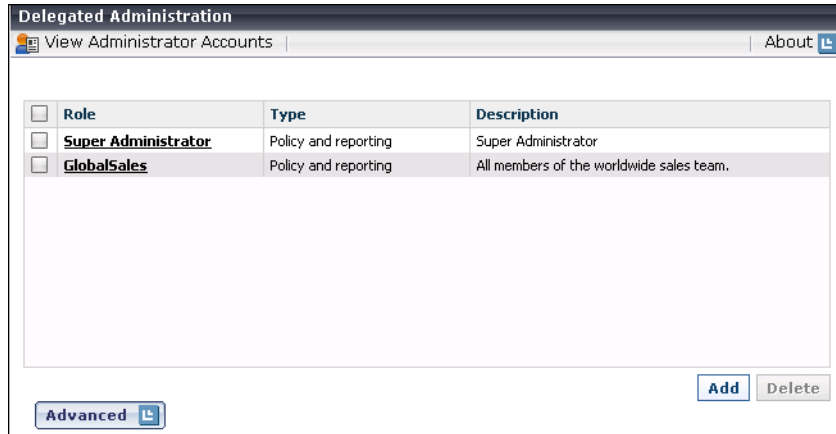
Clients can be added to multiple investigative reporting roles.

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.

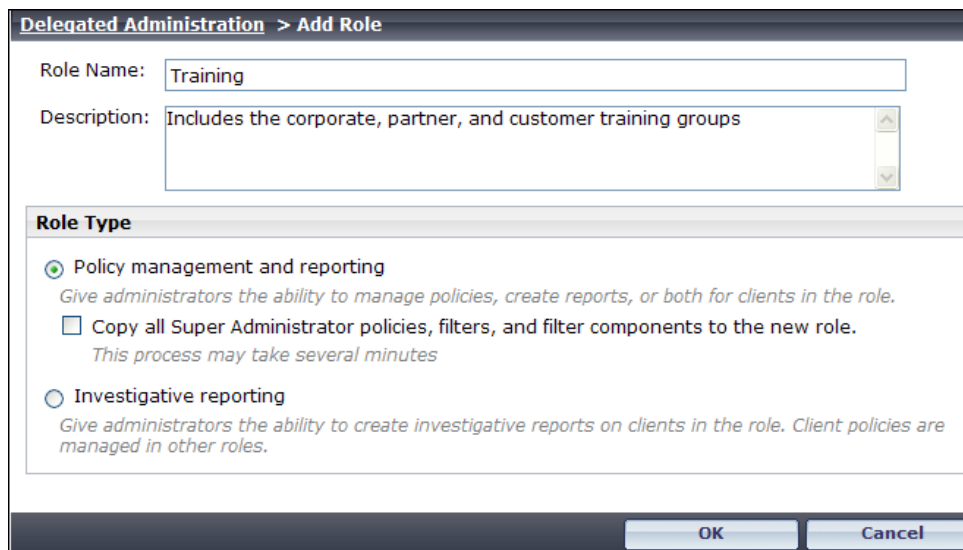
To create a role:

1. In the Web Security manager, go to the **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.

Delegated Administration > Add Role > Edit Role

Name: **Training Rename**

Description: Includes the corporate, partner, and customer training groups

Role type: Policy management and reporting

Administrators

<input type="checkbox"/>	User Name	Account Type	Policy	Reporting	Real-Time Monitor	Audi
<input type="checkbox"/>	Training_Admin	Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Managed Clients

<input type="checkbox"/>	10.132.15.60-10.132.15.85
--------------------------	---------------------------

Add **Add**

Add administrators to the role (v7.6)

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 **Administrator** and **Auditor** radio buttons to indicate which general permissions the selected administrators should have. You can make further refinements later.
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, use the **Policy**, **Reporting**, **Real-Time Monitor**, and **Auditor** check boxes in the Administrators list to edit permissions.

At the bottom of the page, under **Reporting Permissions**, specify which reporting tools administrators with reporting permissions can access.

Reporting Permissions ⓘ

Report on all clients

Report on managed clients only

If administrators are limited to reporting on managed clients only, they are restricted from certain reports on the Today and History pages, and cannot access either presentation reports or the Test Filtering option in the toolbox. You can give these administrators access to investigative reports features.

Access presentation reports

View reports on Today and History pages

Access investigative reports

View user names in investigative reports

Save investigative reports as favorites

Schedule investigative reports

Manage the Log Database

- 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.

Reporting Permissions ⓘ

Report on all clients

Report on managed clients only

If administrators are limited to reporting on managed clients only, they are restricted from certain reports on the Today and History pages, and cannot access either presentation reports or the Test Filtering option in the toolbox. You can give these administrators access to investigative reports features.

Access presentation reports

View reports on Today and History pages

Access investigative reports

View user names in investigative reports

Save investigative reports as favorites

Schedule investigative reports

Manage the Log Database

When you are finished adding administrators, continue with [Add clients to the role](#), page 20.

Add administrators to the role (v7.7 and later)

To add delegated administrators:

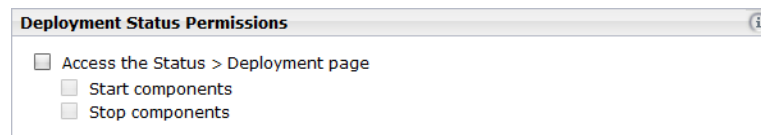
1. Click the **Add** button below the Administrators list.
2. Select administrators to add to the role, and then click the appropriate right-arrow button to add them to the Selected list.
3. If you have created a *policy management and reporting* role, use the **Policy management**, **Reporting**, and **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.

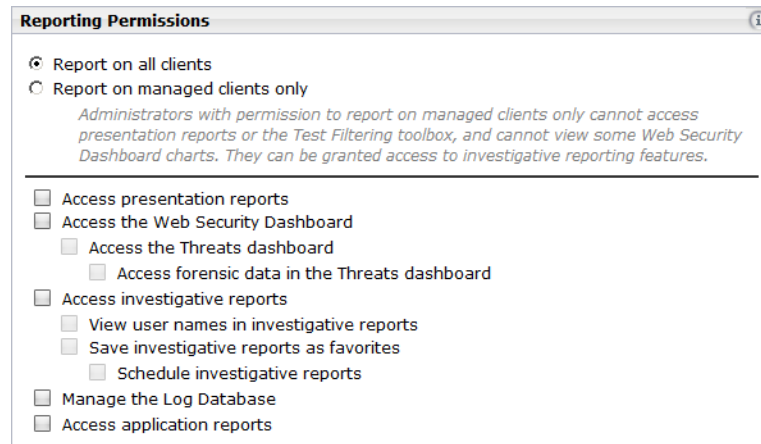
If you have created an *investigative reporting* role, there are no permissions to configure on this page.

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.

In version 7.8, 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.

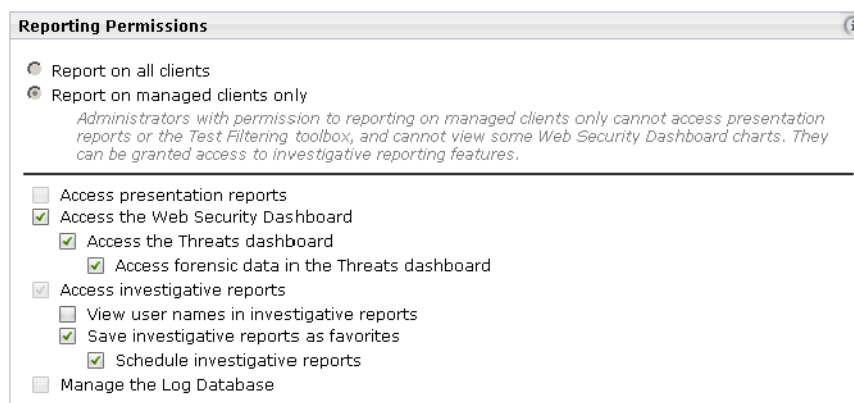


For all versions, under **Reporting Permissions**, specify which reporting tools administrators with reporting permissions can access.



Note that the option to access application reports is available only in v7.8 and later.

- 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 20.

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 Web Security 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

Topic 50208 | Delegated Administration Quick Start | Updated 22-Oct-2013

Applies to:	Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.6, 7.7, and 7.8
--------------------	---

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

1. Access the TRITON console (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. (v7.7 and later) 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 (v7.8) or New User Quick Start tutorial (v7.7 and earlier) and the Web Security Help for your version. Both the Quick Start and the Help can be accessed from the Help menu in the Web Security manager, or from support.websense.com.

In version 7.8, the Find Answers box in the right, shortcut pane also provides links to relevant information.