Delegated Administration Quick Start

Delegated administration is a powerful tool for distributing filtering and reporting responsibilities across an organization.

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

- Create a set of master filtering restrictions that limit the filtering access that delegated administrators can provide.
- Send copies of policies and filters that they have created to delegated administrators, who can use these policies 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 and reporting on their Internet usage. For example, a school district might create Staff, Teachers, and Elementary Students roles, and then assign one or more administrators to each.

Overview

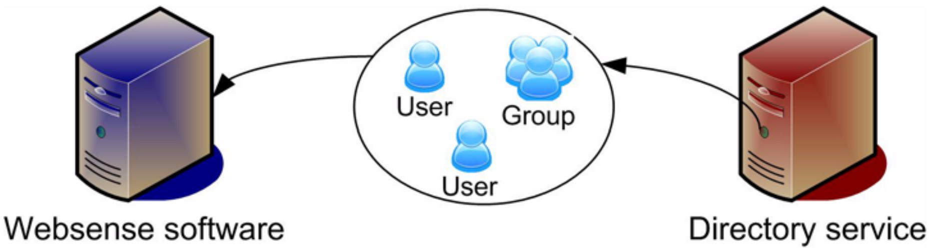
To start using delegated administration:

- ❑ Configure Websense software to communicate with your directory service so that you can add user, group, and domain (OU) clients in TRITON - Web Security.
- ❑ Configure TRITON - Web Security to communicate with one directory server to authenticate administrative logons.
- ❑ Customize the Default category and protocol filters to establish a filtering baseline for your organization.
- ❑ Modify the Filter Lock to enforce basic category and protocol filtering restrictions that will apply to all delegated administrators.
- ❑ Create Websense user accounts for any administrators who will not log on using their network logons.
- ❑ Create roles, and assign administrators and clients to each one.
- ❑ Train delegated administrators 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 TRITON - Web Security Help, available in HTML or PDF format from the Help menu in TRITON - Web Security.

1. Configure directory service settings

In order for Websense software to filter and report on Internet usage by users, groups, and domains (OUs) defined in your directory service, you must first configure Websense software to communicate with the directory.



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

Websense software can communicate with Windows NT Directory, Windows Active Directory (native or mixed mode), Novell eDirectory, and Sun Java System Directory Server.

To configure directory service settings in TRITON - Web Security:

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 *Clients* topic in the TRITON - Web Security Help 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 TRITON - Web Security, and then re-add them.

2. Configure administrator logon directory settings

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

If you prefer that administrators use only local Websense accounts, you can skip this section.

1. In TRITON - Web Security, click the **Settings** tab of the left navigation pane, and then select **Logon Directory**.
2. Mark the **Use a directory service...** check box.
3. Select an entry from the **Directory service** drop-down list.
4. Do one of the following:

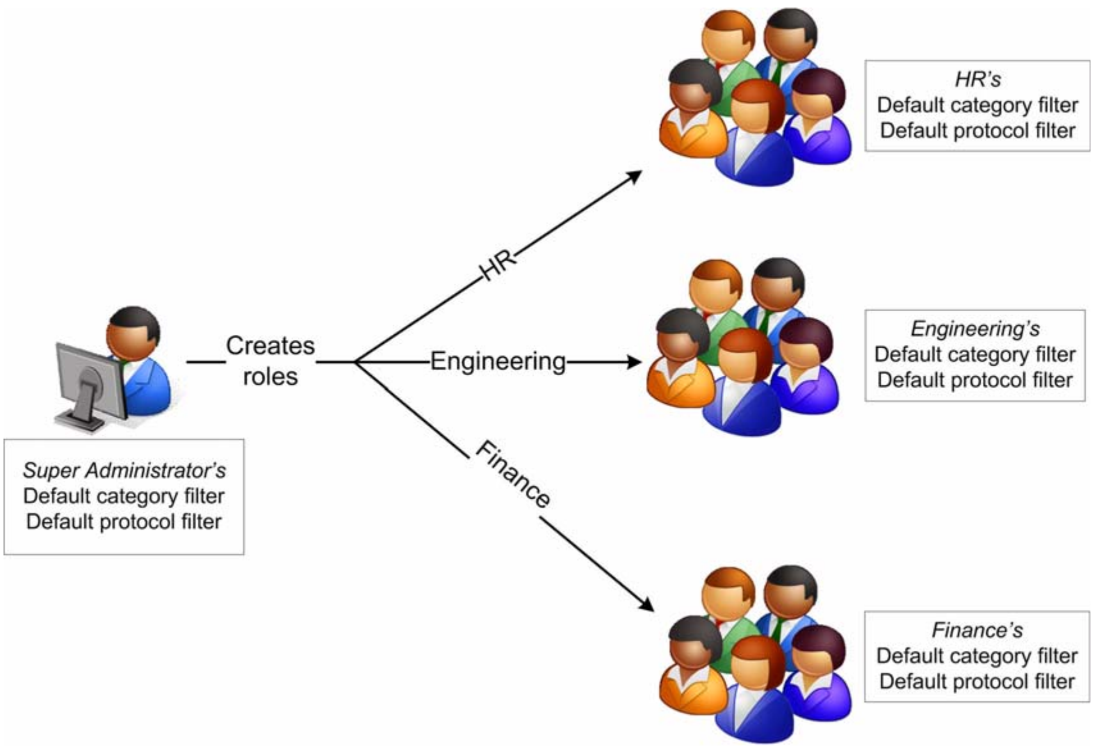
- If the directory service that will be used to authenticate administrator logons is **the same** directory service that you are using to identify directory clients, click **Get Settings**.

The settings that you configured on the Settings > Directory Services page are copied to the Logon Directory page. If you are using Windows Active Directory (Native Mode), and have configured communication with multiple global catalog servers, only the first server IP address or host name is copied to the Logon Directory page.

- If the directory service that will be used to authenticate administrator logons is **different from** the directory service that you are using to identify directory clients, provide configuration information as prompted. Refer to the *Delegated Administration* section of the TRITON - Web Security Help for detailed instructions.

3. Customize the Default category and protocol filters

When you create delegated administration roles, 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.



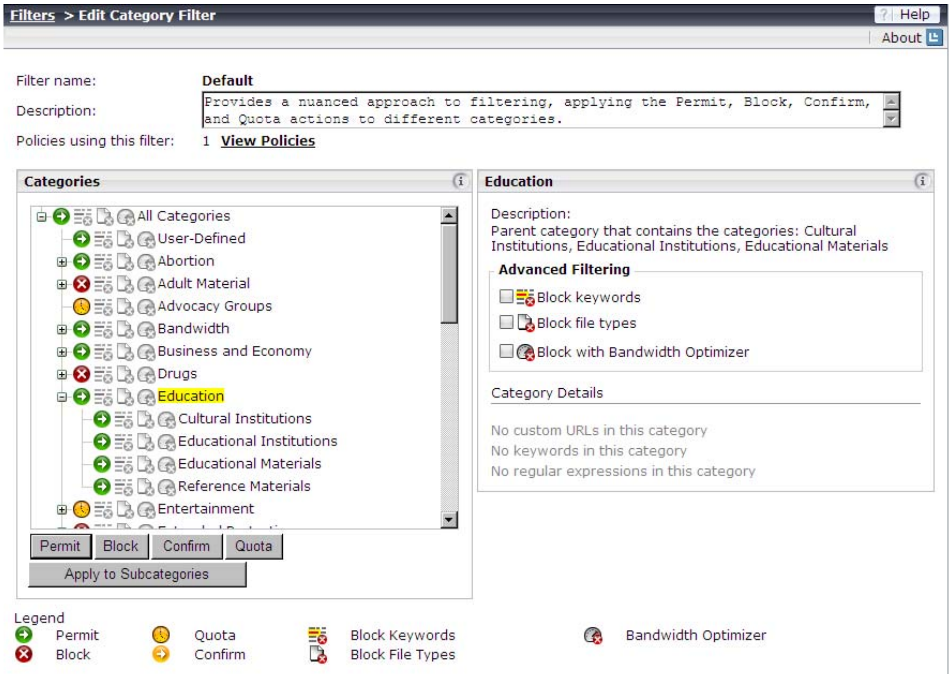
Changes made to the Default filters in the Super Administrator role are not automatically reflected in the Default filters in other roles. After delegated administration roles have been created, however, any Super Administrator can:

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

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

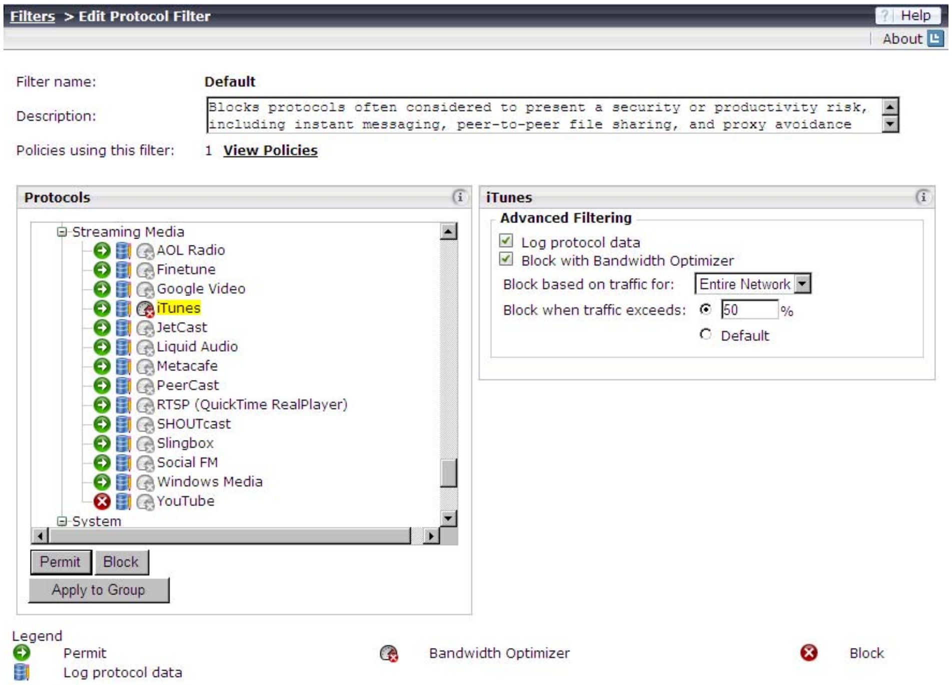
1. In TRITON - Web Security, on the **Main** tab of the left navigation pane, select **Filters**.

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**.

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

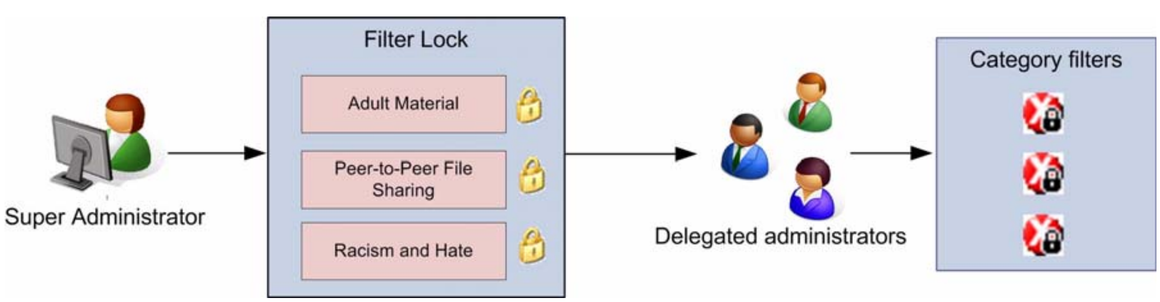


6. Scroll through the Protocols list to ensure that the appropriate action is applied to each protocol.
   - To change the action applied to a protocol, use the buttons at the bottom of the list.
   - You can also use the Advanced Filtering check boxes to the right of the Protocols list to change logging 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**.

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

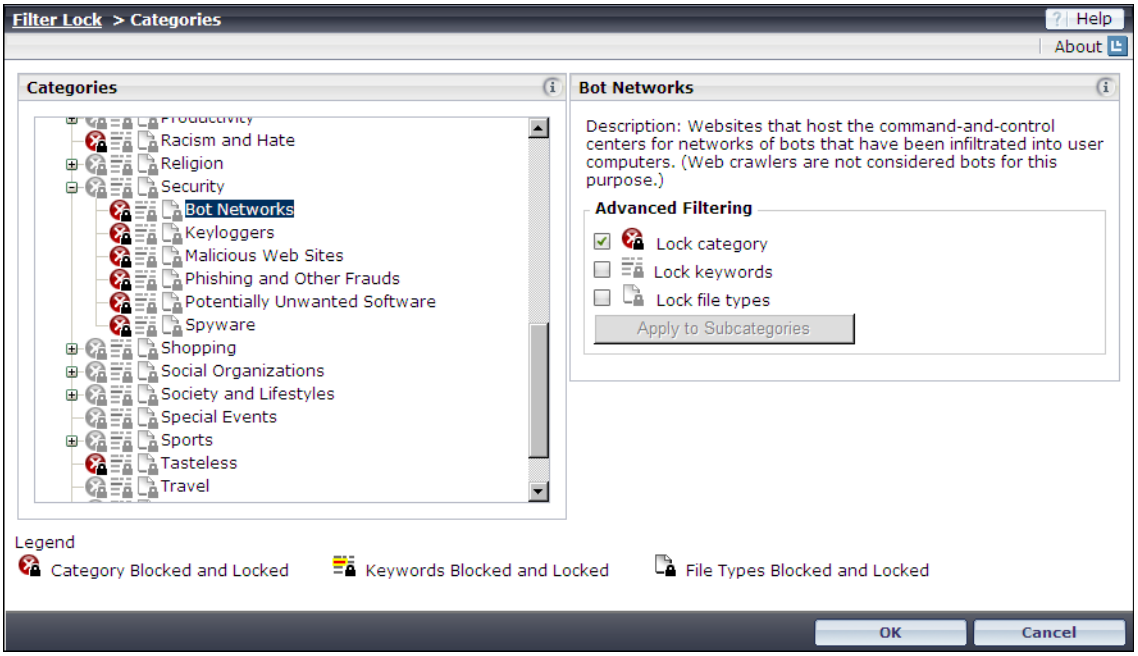
4. Edit the Filter Lock

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.

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.

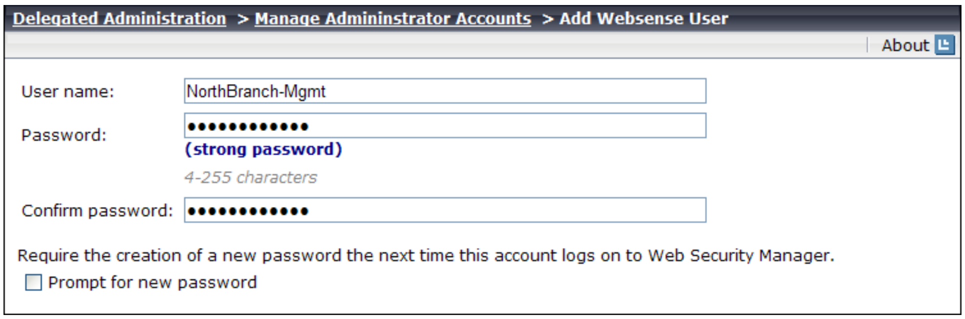
   These settings affect all category filters managed by delegated administrators in all roles (excluding the Super Administrator role).
5. Repeat for each additional category that you want to lock.
6. When you are finished making changes, click **OK** to return to the Filter Lock page.
7. Under the Manage 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** to implement your changes to the Filter Lock.

5. Create Websense user accounts

You can use TRITON - Web Security to create local logon accounts for administrative users. These accounts are not authenticated against your network's directory service, and are used only for managing Websense software.

If you are using network logon accounts exclusively, you can skip this section.

1. On the **Main** tab of the left navigation pane, go to **Policy Management > Delegated Administration**.
2. Click **Manage Administrator Accounts** at the top of the page.
3. Under Websense User Accounts, click **Add**.



4. Enter a unique **User name**, up to 50 characters, for the new logon account.

   The name must be between 1 and 50 characters long, and cannot include any of the following characters:

   `* < > ' { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,`

   User names can include spaces and dashes.
5. Enter and confirm a **Password** for the account.
   - The password must be between 4 and 255 characters.
   - Strong passwords are recommended: 8 characters or longer, including at least one uppercase letter, lowercase letter, number, and special character (such as hyphen, underscore, or blank).
6. Indicate whether or not to prompt the administrator for a new password the first time the account is used to log on to TRITON - Web Security.
7. Click **OK** to cache your changes and return to the Manage Administrator Accounts page. Changes are not implemented until you click **Save All**.

Repeat this process to create additional administrative accounts, as needed.

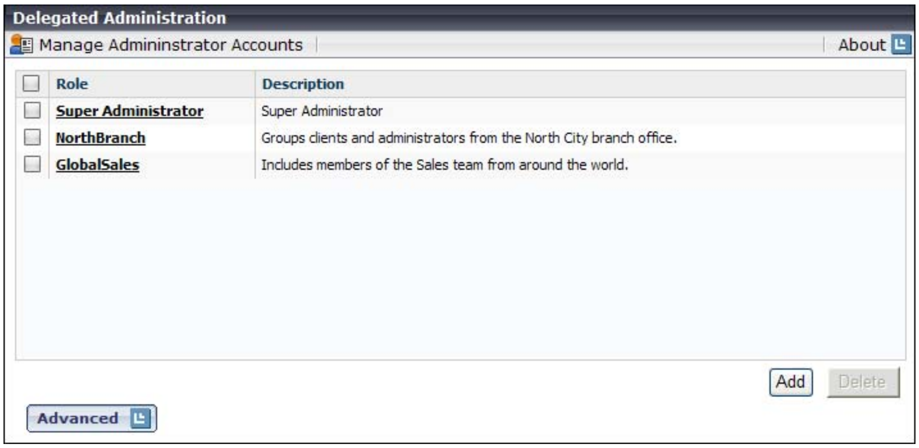
6. Create delegated administration roles

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. A role can include multiple administrators, and different administrators within a role can have different privileges. For example, the Intern 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 only those clients not assigned to a delegated administration role, but they can report on clients in all roles.

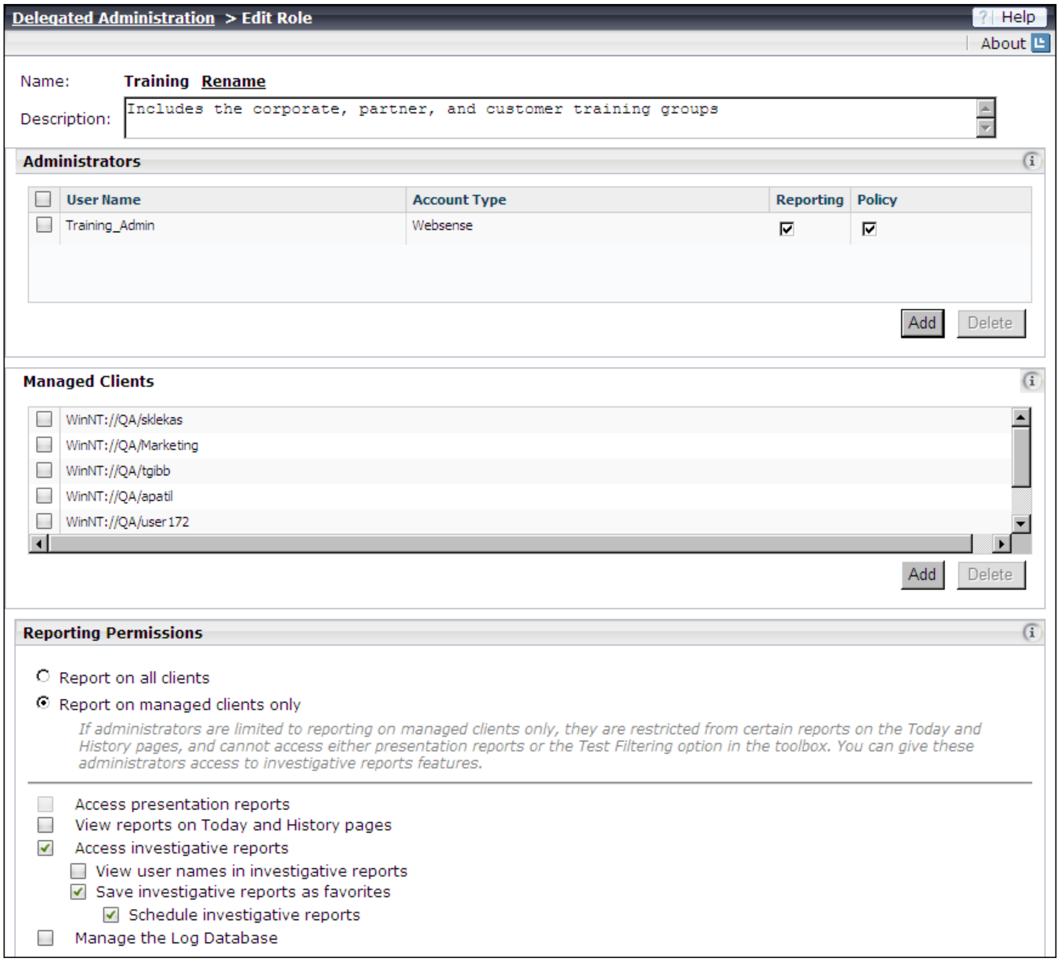
To create a role:

1. On the **Main** tab of the left navigation pane, click **Delegated Administration** (under Policy Management). A list of existing roles is displayed. Initially, this shows only the Super Administrator role.



2. Click **Add**.

3. Provide a name and description for the new role, and then click **OK** to go to the Edit Role page.



To add administrators to the role:

1. Click the **Add** button below the Administrators list to add one or more delegated administrators to this role.
2. Select administrators to add to the role, and then click the appropriate right-arrow button to add them to the Selected list.
   - Mark the check box next to any Websense user account that you want to give administrative permissions in this role.
   - Click **New Websense User** or **New Network Account** to add an administrator not already listed.
3. Use the **Policy** and **Reporting** check boxes to indicate which general permissions the selected administrators should have. You can make further refinements later.
4. Click **OK** to return to the Edit Role page.
5. To change an administrator's policy and reporting management permissions:
   - Use the **Policy** and **Reporting** check boxes in the right portion of the Administrators list to add or remove permissions.

- Use the **Reporting Permissions** radio buttons and check boxes at the bottom of the page to further refine how administrators with reporting privileges use reporting tools.

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. IP addresses and ranges cannot overlap IP addresses and ranges already added to other roles.
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** to implement your changes.

7. Train delegated administrators

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

- ❑ Access TRITON - Web Security (both the URL, and which logon account to use)
- ❑ Select the appropriate role (for those managing more than one role)
- ❑ Create filters and policies
- ❑ Add managed clients to their Clients page and assign them a policy
- ❑ Access reporting tools to generate and schedule reports

Detailed instructions for performing common policy and reporting tasks are available in the New User Quick Start tutorial and the TRITON - Web Security Help. Both can be accessed from the Help menu in TRITON - Web Security, or from the Websense Knowledge Base.

8. Further resources

Refer to the TRITON - Web Security Help, available from within TRITON - Web Security or from the Websense Knowledge Base, for detailed information about delegated administration.

The TRITON - Web Security Help includes information for delegated administrators about how to manage filtering and reporting for clients in the role or roles that they manage.

The Websense Knowledge Base is located at kb.websense.com.