Yes!

websense®

ESSENTIAL INFORMATION PROTECTION™

Making best use of Websense Web Security delegated administration and reporting

Webinar February 2012

web security | data security | email security

Webinar Presenter

Greg Didier

- Title: Support Specialist
- Accomplishments:
  - 9 years supporting Websense products
- Qualifications:
  - Technical Support Mentor
  - Product Trainer

Goals And Objectives

- Delegated administration fundamentals
  - Administration accounts
  - Roles
  - Permissions
- Implementation
- Real world scenarios
- Best practice tips
- Demonstrations

Delegated Administration

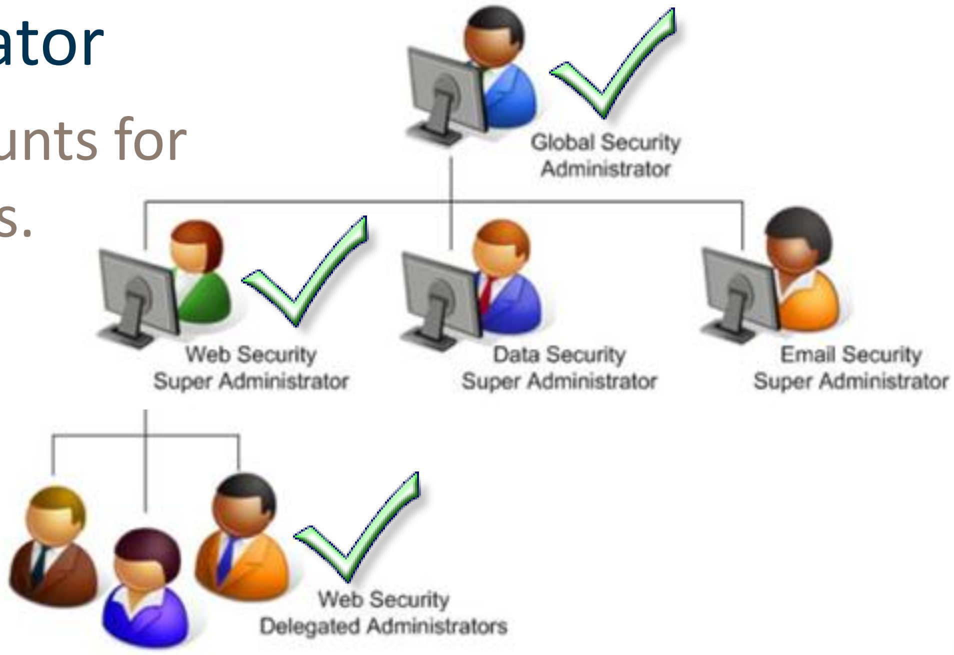
- Delegated administration allows for distributing filtering configuration, policy management, and reporting responsibilities across an organization.
- Accomplished by employing:
  - Administrators
  - Roles
  - Permissions

The Three Concepts

- **Administrators**
  - Configure TRITON - Web Security settings, manage client policies, run Internet activity reports, or audit the system.
- **Roles**
  - Are the containers that group related clients with administrators responsible for policy management, reporting, or both.
- **Permissions**
  - Determine what responsibilities an administrator has within a role.

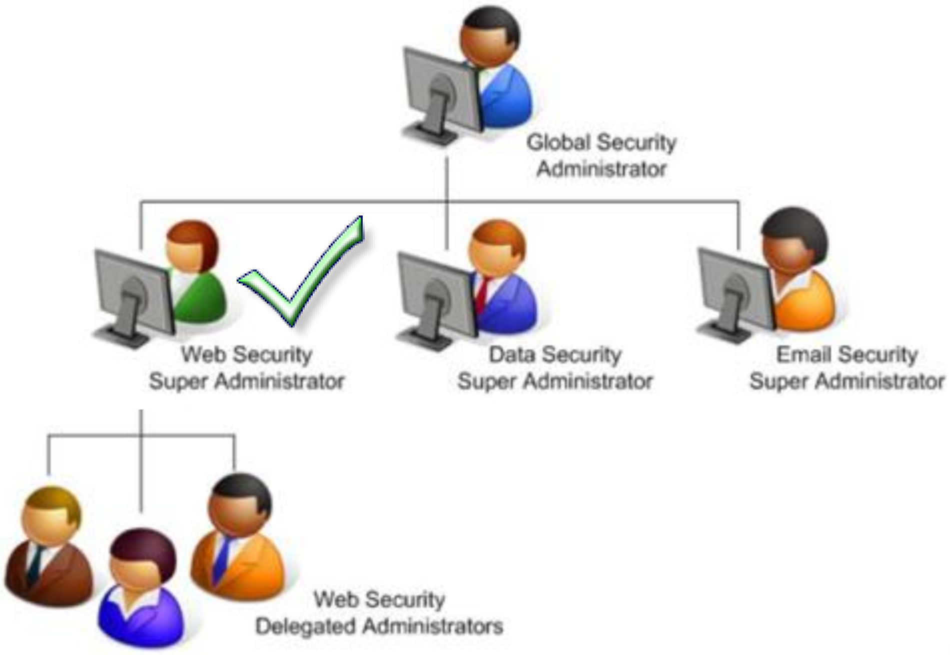
Administrators

- Three administrator types
  - Global Security Administrator
  - Super Administrator
  - Delegated administrator
- The accounts differ in what actions they can perform.
- Global Security Administrator
  - Create administrative accounts for all TRITON console modules.


Global Security Administrator
Web Security Super Administrator
Data Security Super Administrator
Email Security Super Administrator
Web Security Delegated Administrators

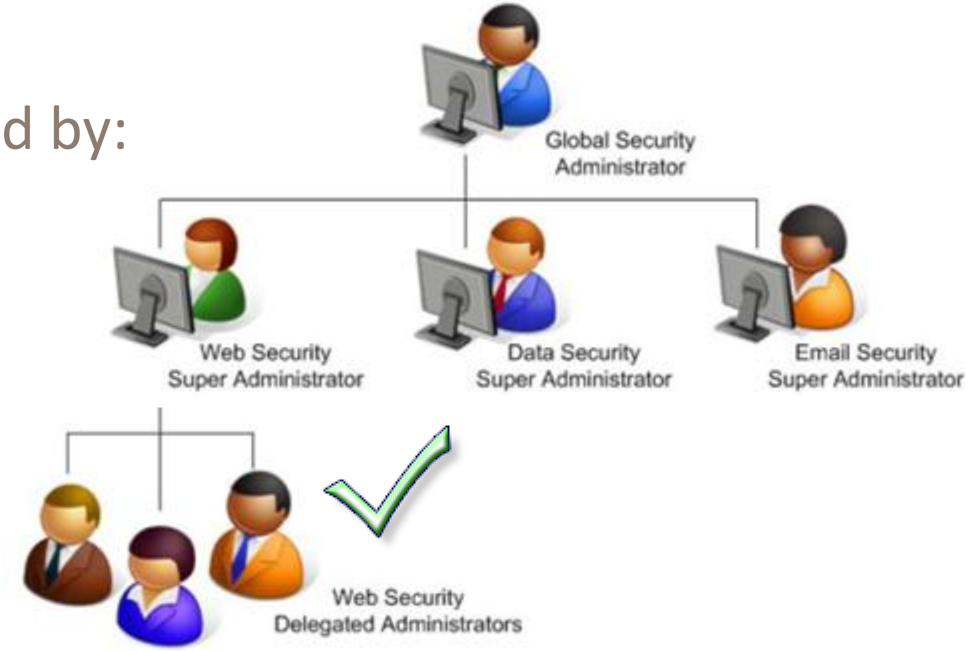
Administrators

- Super Administrator
  - Have unconditional permissions within a Security module.
  - Set filtering change restrictions on delegated administrators.
  - Create delegated administration roles.
  - Assign delegated administrators and clients to roles.
  - Grant policy management, reporting rights, or both.


Global Security Administrator
Web Security Super Administrator
Data Security Super Administrator
Email Security Super Administrator
Web Security Delegated Administrators

Administrators

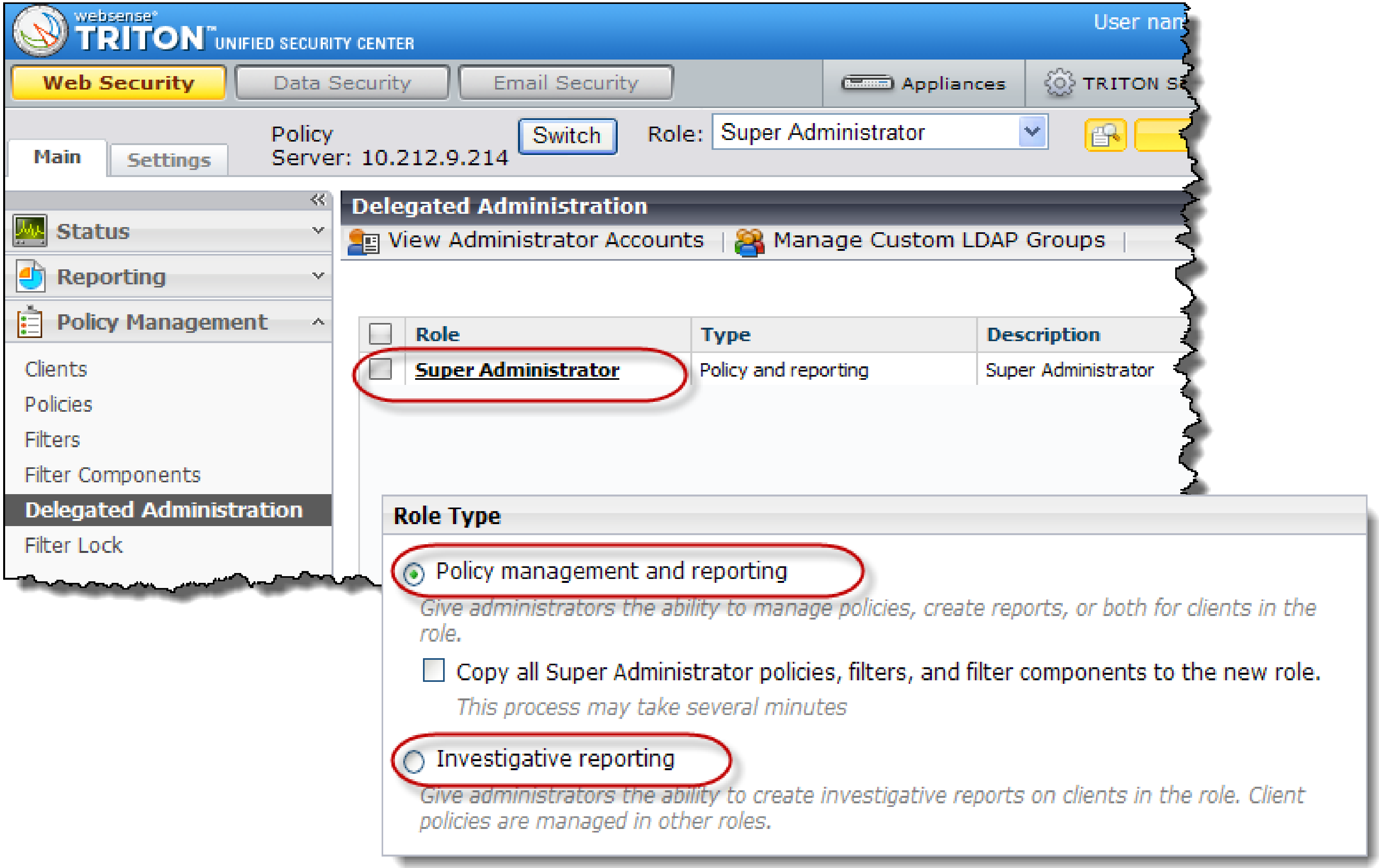
- Delegated administrator
  - Has policy management or reporting permissions, or both.
    - Role type 1: *Policy and reporting*
    - Role type 2: *Reporting only*
  - Manage specific clients assigned to the role.
    - Clients defined within a role are referred to as *managed clients*.
  - Actions allowed are defined by:
    - Role type
    - Permissions
  - *"Use this account type for delegated administration."*


Global Security Administrator
Web Security Super Administrator
Data Security Super Administrator
Email Security Super Administrator
Web Security Delegated Administrators

Role Types

- *Super Administrator* role
  - Primary predefined default role, cannot be deleted.
  - Only one Super Administrator role.
  - Users in this role can create and manage delegated roles.
- *Policy management and reporting* role
  - Allows assigning delegate policy and reporting permissions.
  - Typically, you assign auditors to this role.
  - Managed clients can belong to one policy management role.
- *Investigative reporting* role
  - Limits administrators to reporting permissions only.
  - May contain managed clients from other reporting or policy roles.

Role Types



Policy Server: 10.212.9.214

Role: Super Administrator

Delegated Administration

□	Role	Type	Description
□	Super Administrator	Policy and reporting	Super Administrator

Role Type

● Policy management and reporting

Give administrators the ability to manage policies, create reports, or both for clients in the role.

□ Copy all Super Administrator policies, filters, and filter components to the new role.

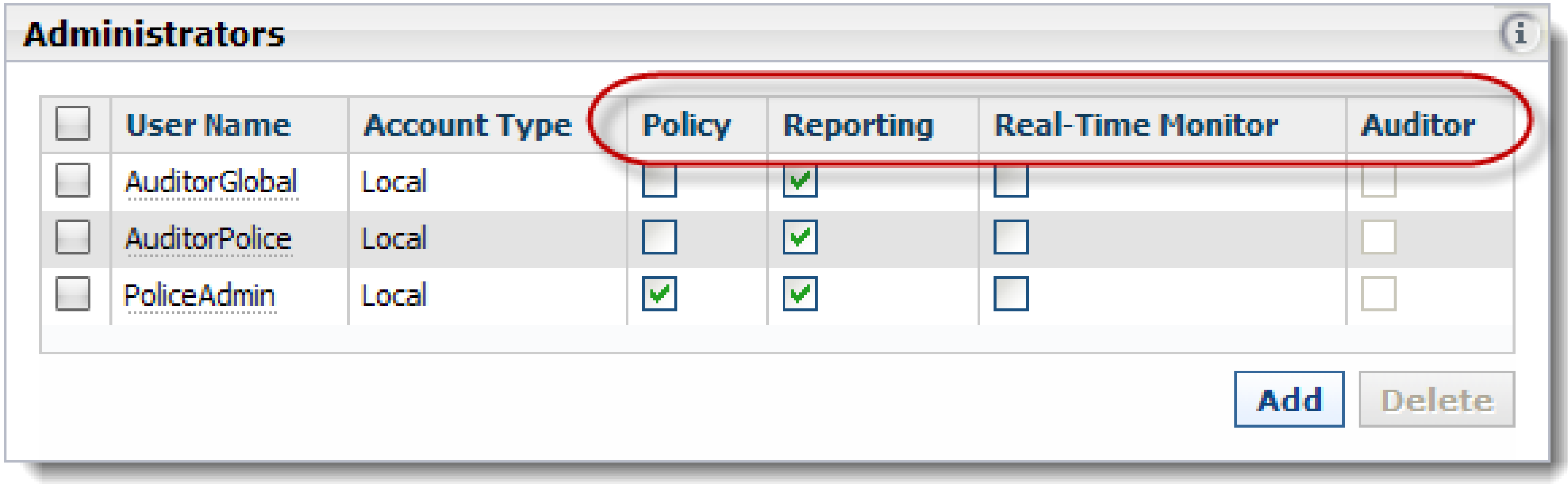
This process may take several minutes

○ Investigative reporting

Give administrators the ability to create investigative reports on clients in the role. Client policies are managed in other roles.

Permissions

- Permissions available depend on the assigned role type.
  - *Super Administrator* role
  - *Policy management and reporting* role
  - *Investigative reporting* role
- Delegated administrators in a role can be given a combination of permissions.

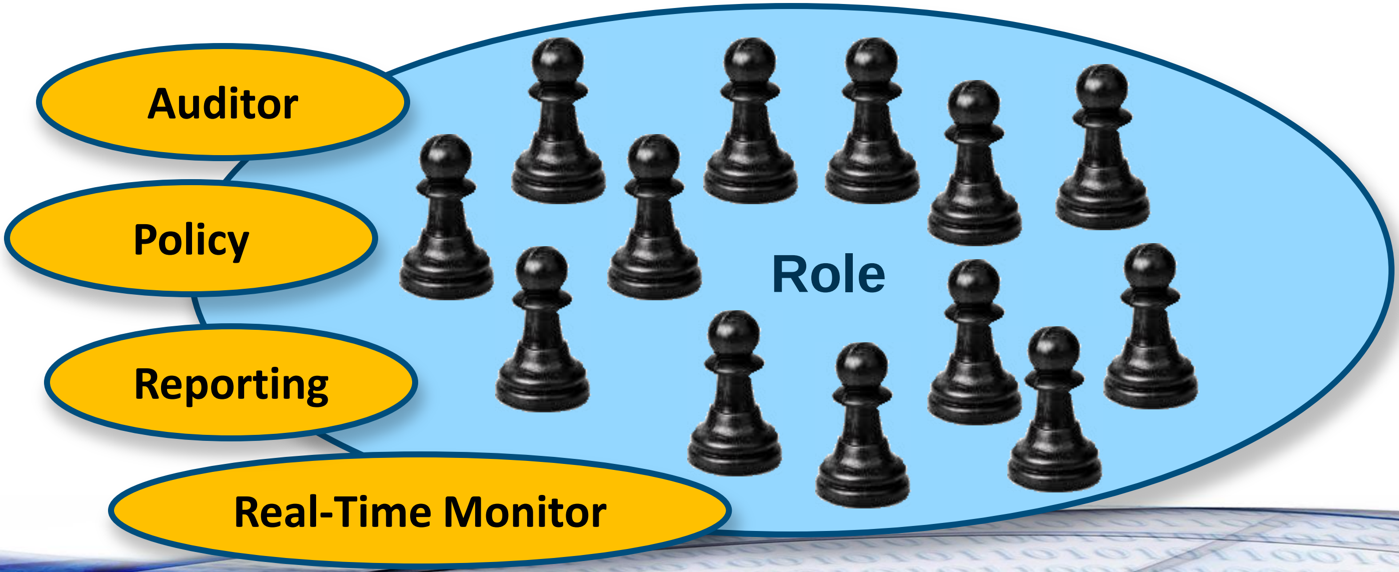


Administrators

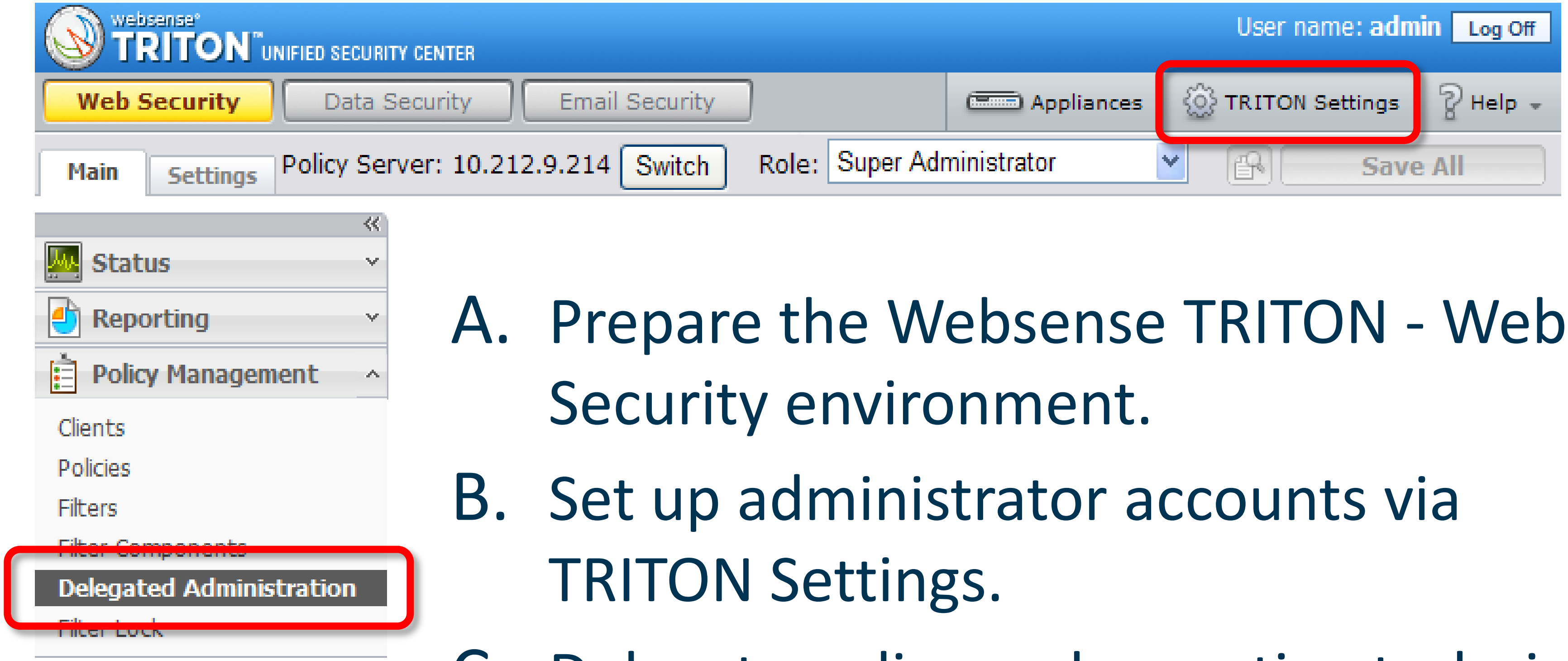
□	User Name	Account Type	Policy	Reporting	Real-Time Monitor	Auditor
□	AuditorGlobal	Local	□	☑	□	□
□	AuditorPolice	Local	□	☑	□	□
□	PoliceAdmin	Local	☑	☑	□	□

Implementing Delegated administration

- Web Security, Super Administrator
  - Creates a role.
    - Policy and reporting, or reporting only.
  - Defines role permissions.
  - Creates a delegated administrator.
  - Assigns a delegated administrator to a role.
  - Assigns managed clients to a role.



Implementation – Three Phases



User name: admin

Policy Server: 10.212.9.214

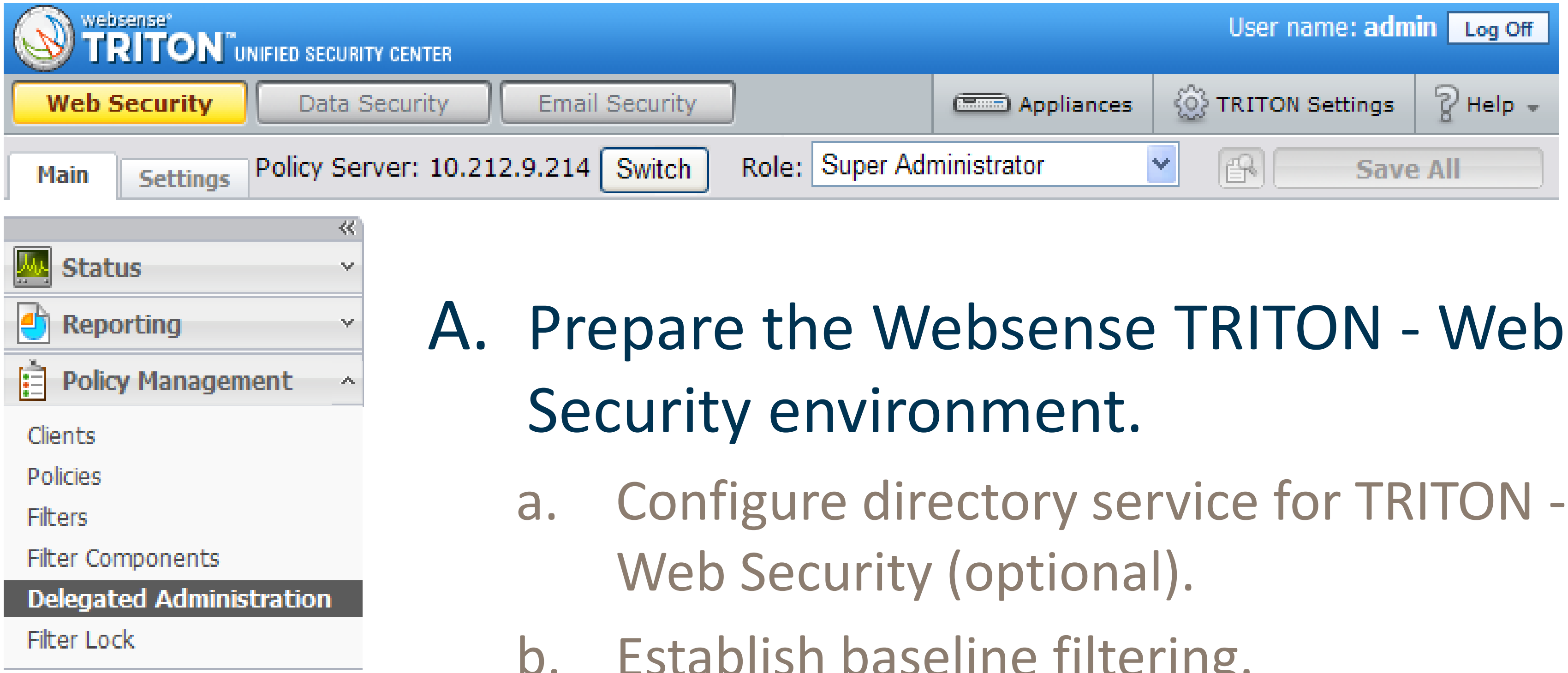
Role: Super Administrator

A. Prepare the Websense TRITON - Web Security environment.

B. Set up administrator accounts via TRITON Settings.

C. Delegate policy and reporting tasks in TRITON - Web Security.

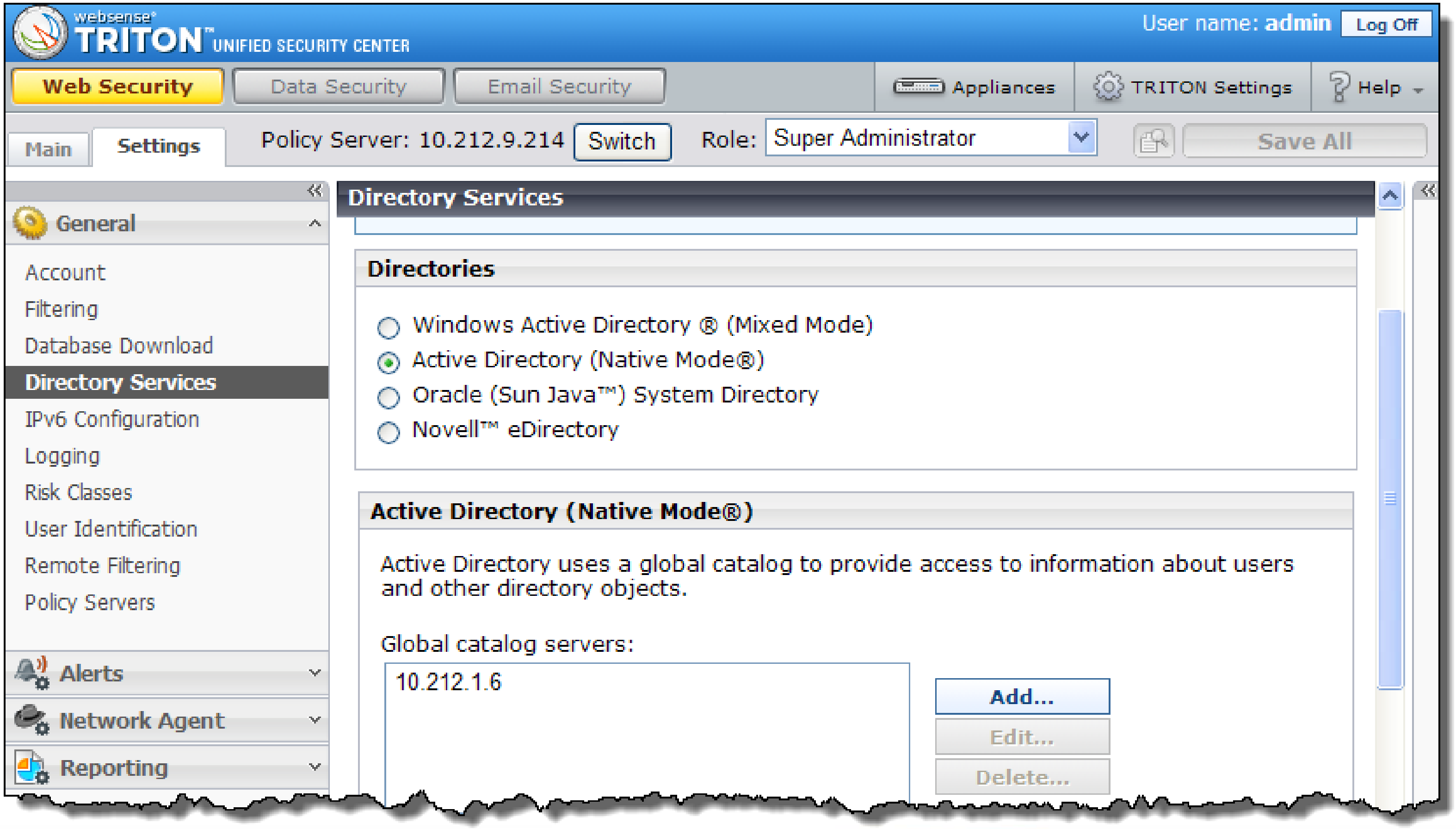
Implementation – Phase One



A. Prepare the Websense TRITON - Web Security environment.
   a. Configure directory service for TRITON - Web Security (optional).
   b. Establish baseline filtering.
   c. Create category and protocol filtering restrictions.

TRITON Directory Services

- Required to filter and report by users and groups.
- Not required if filtering on IP addresses.



Policy Server: 10.212.9.214

Role: Super Administrator

Directory Services

Directories

○ Windows Active Directory ® (Mixed Mode)
● Active Directory (Native Mode®)
○ Oracle (Sun Java™) System Directory
○ Novell™ eDirectory

Active Directory (Native Mode®)

Active Directory uses a global catalog to provide access to information about users and other directory objects.

Global catalog servers:

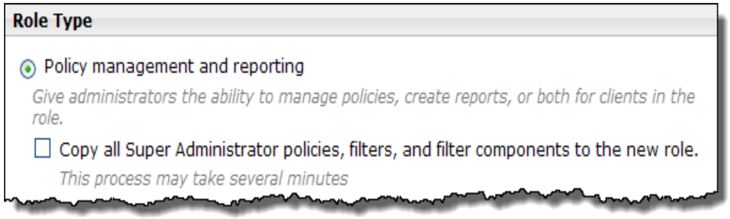
10.212.1.6

Baseline Filtering

- Best practice.
  - Super Administrator policies and filters should provide a useful baseline for delegated administrators.
  - At least, the Super Administrator should review the Default filters.
  - Remember, delegated administrators can edit policies and filters within their roles, and create new policies and filters.
- Future policies changes made in the Super Administrator role are not conveyed to other roles.
- After a role has been created, Super Administrator can:
  - Use the Copy to Role option.
  - Copy additional policies and filters to delegated role.

Establish Baseline Filtering

- Configuration items are copied from Super Administrator role to the new delegated administration role.
  - By default, only the Default category and protocol filters copy.
  - Optionally, you may copy all policies, filters, custom categories, custom URLs, and keywords.



Role Type

● Policy management and reporting

Give administrators the ability to manage policies, create reports, or both for clients in the role.

□ Copy all Super Administrator policies, filters, and filter components to the new role.

This process may take several minutes

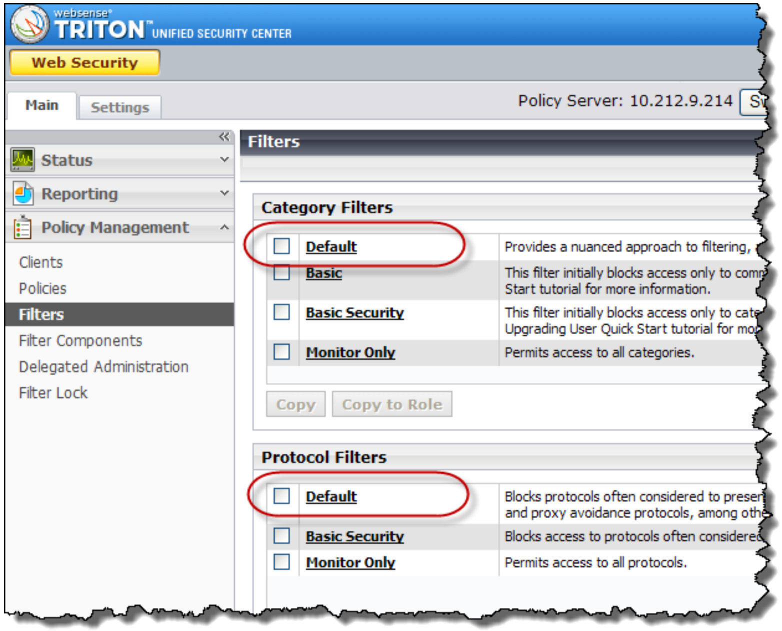
Creates Role → New Administration Role

Super Administrator's
- Default category filter
- Default protocol filter

→

New role's Default policy:
- Default category filter
- Default protocol filter

Establish Baseline Filtering



websense® TRITON™ UNIFIED SECURITY CENTER

Policy Server: 10.212.9.214

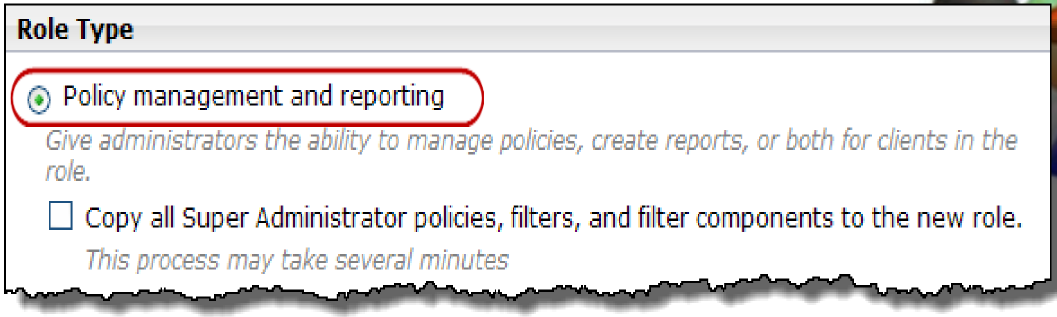
Filters

Category Filters

□ Default	Provides a nuanced approach to filtering,
□ Basic	This filter initially blocks access only to comp Start tutorial for more information.
□ Basic Security	This filter initially blocks access only to cate Upgrading User Quick Start tutorial for mo
□ Monitor Only	Permits access to all categories.

Protocol Filters

□ Default	Blocks protocols often considered to preser and proxy avoidance protocols, among oth
□ Basic Security	Blocks access to protocols often considered
□ Monitor Only	Permits access to all protocols.



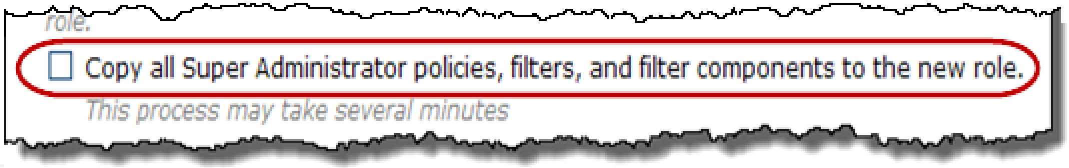
Role Type

● Policy management and reporting

Give administrators the ability to manage policies, create reports, or both for clients in the role.

□ Copy all Super Administrator policies, filters, and filter components to the new role.

This process may take several minutes

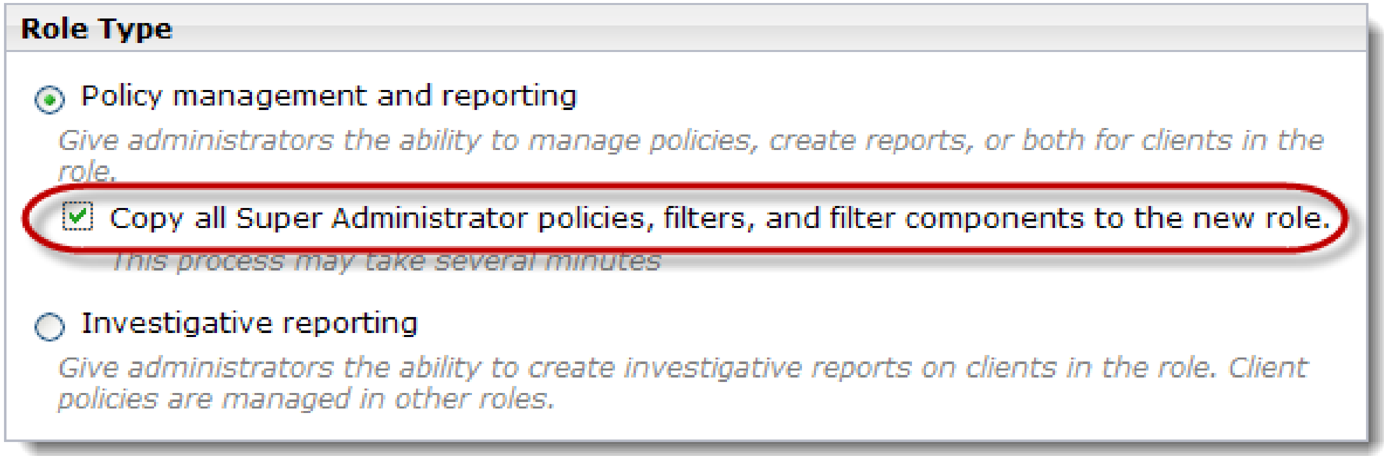


role.

□ Copy all Super Administrator policies, filters, and filter components to the new role.

This process may take several minutes

Establish Baseline Filtering



Role Type

● Policy management and reporting

Give administrators the ability to manage policies, create reports, or both for clients in the role.

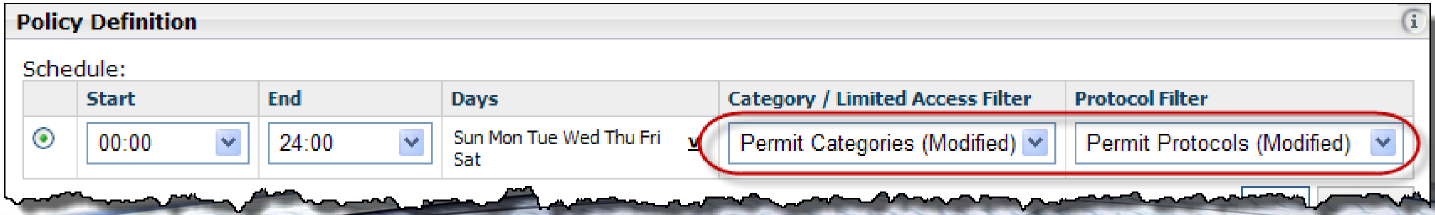
☑ Copy all Super Administrator policies, filters, and filter components to the new role.

This process may take several minutes

○ Investigative reporting

Give administrators the ability to create investigative reports on clients in the role. Client policies are managed in other roles.

- NOTE: A new filter is created for policies containing the Permit All filter.
  - The new filter permits all categories or protocols not blocked and locked by the Filter Lock.
  - The new filter names:



Policy Definition

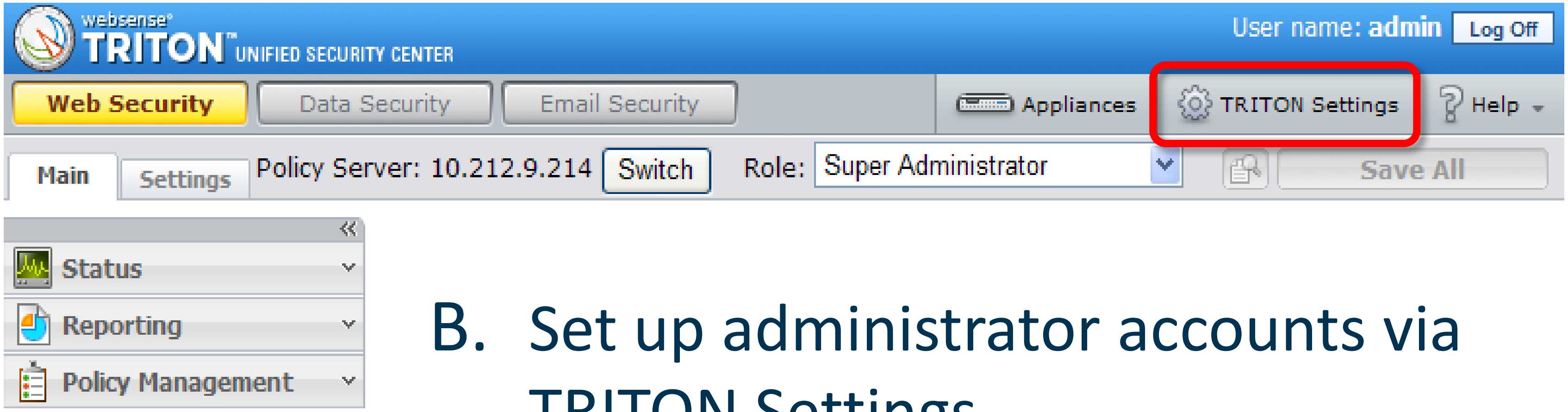
Schedule:

	Start	End	Days	Category / Limited Access Filter	Protocol Filter
●	00:00	24:00	Sun Mon Tue Wed Thu Fri Sat	Permit Categories (Modified)	Permit Protocols (Modified)

Establish Filtering Restrictions

- Filter Lock stops delegated administrators from permitting specific categories and protocols.
- Filter Locks affect all category and protocol filters in every delegated role.
- Super Administrators create and manage Filter Locks.
- Clients managed by the Super Administrator role can access categories and protocols blocked and locked for clients managed in other delegated roles.
  - Filter Locks do not affect clients in the Super Administrator role.

Implementation – Phase Two



Policy Server: 10.212.9.214

Role: Super Administrator

B. Set up administrator accounts via TRITON Settings.

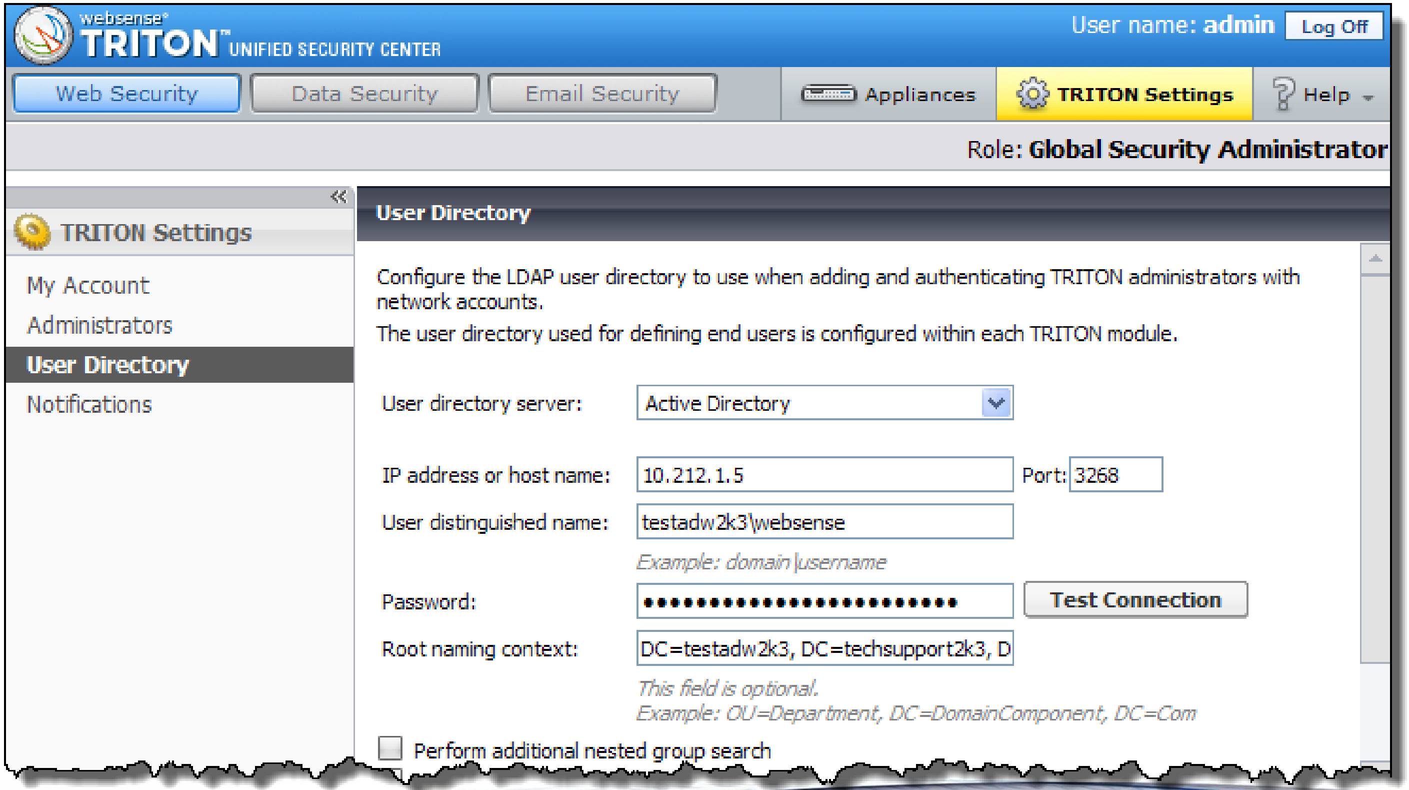
a. Configure directory service for adding administrators (optional).

b. Configure email settings for administrators.

c. Grant administrators access permissions.

Adding Administrators

- Administrative users can log on to the TRITON console using either local accounts or their network accounts.
  - To use network logons, configure TRITON Unified Security Center to communicate with a your directory service.



User Directory

Configure the LDAP user directory to use when adding and authenticating TRITON administrators with network accounts.
The user directory used for defining end users is configured within each TRITON module.

User directory server: Active Directory

IP address or host name: 10.212.1.5 Port: 3268

User distinguished name: testadw2k3\websense

Example: domain\username

Password: ••••••••••••••••••••••••• Test Connection

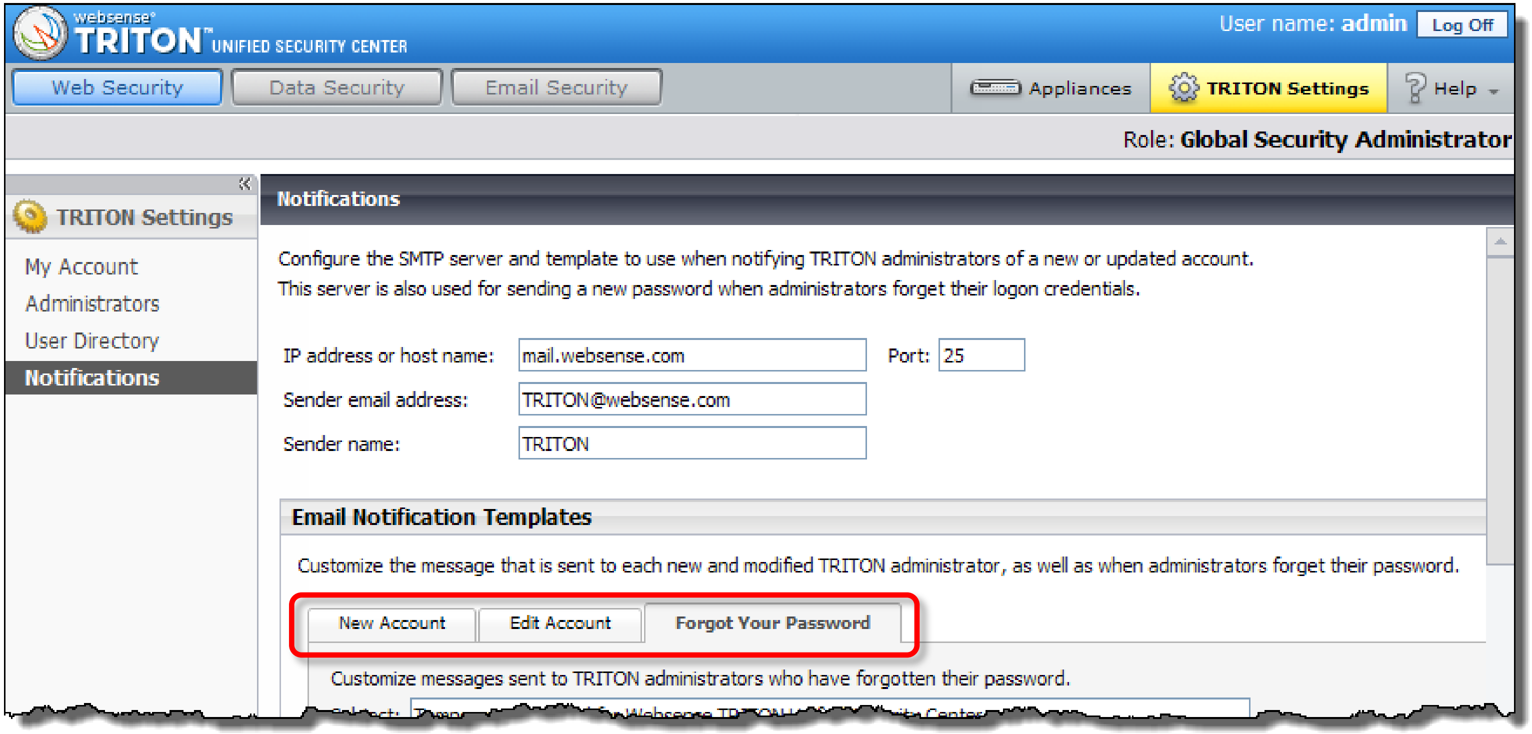
Root naming context: DC=testadw2k3, DC=techsupport2k3, D

This field is optional.
Example: OU=Department, DC=DomainComponent, DC=Com

□ Perform additional nested group search

Administrator Email Settings

- Each administrator account requires an email address.
  - Email address allows sending notifications for:
    - New account access, account changes, and password recovery.



Role: **Global Security Administrator**

Notifications

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.

IP address or host name: mail.websense.com Port: 25

Sender email address: TRITON@websense.com

Sender name: TRITON

Email Notification Templates

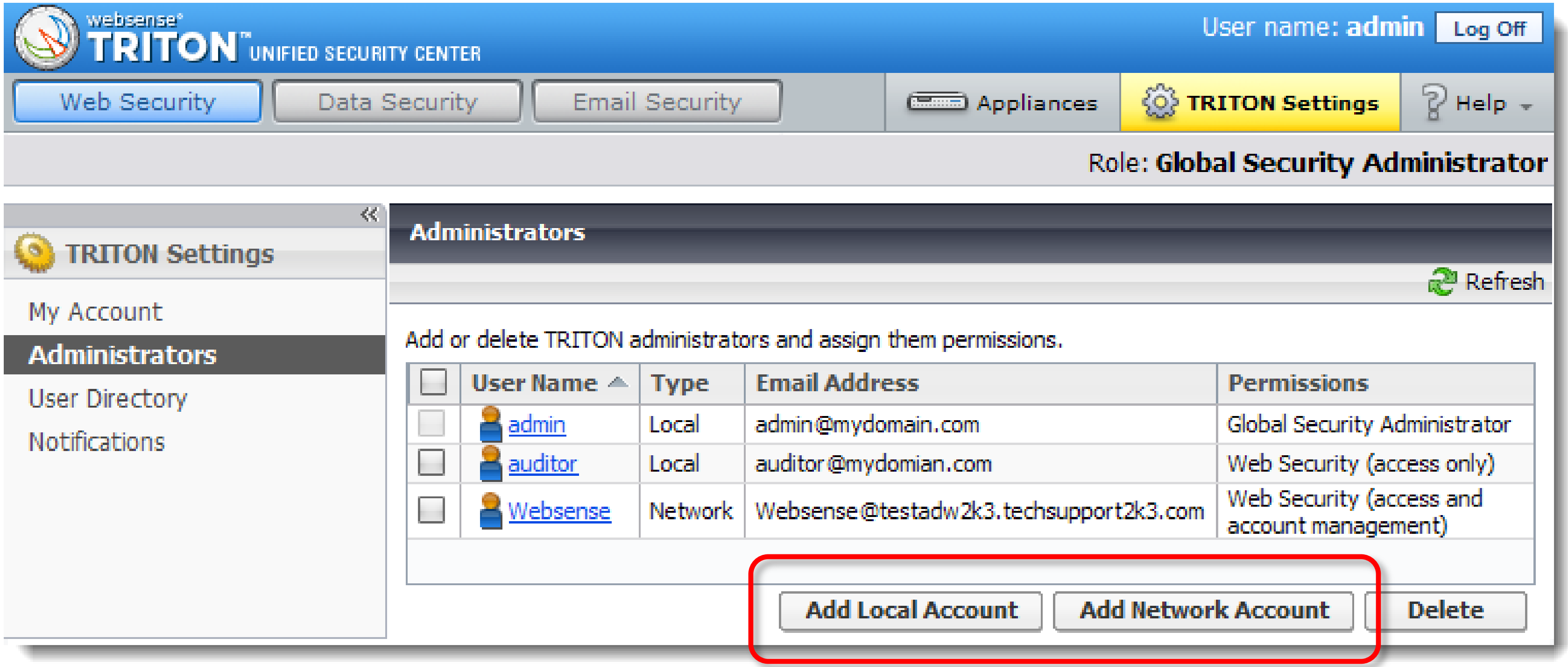
Customize the message that is sent to each new and modified TRITON administrator, as well as when administrators forget their password.

Customize messages sent to TRITON administrators who have forgotten their password.

Subject: [illegible] for Websense TRITON [illegible] Center

Administrator Access Permissions

- Administrator accounts are centrally created and maintained in TRITON Settings.
  - Web Security delegated administrators accounts are not available until they have been added in **TRITON Settings**.



Role: **Global Security Administrator**

Add or delete TRITON administrators and assign them permissions.

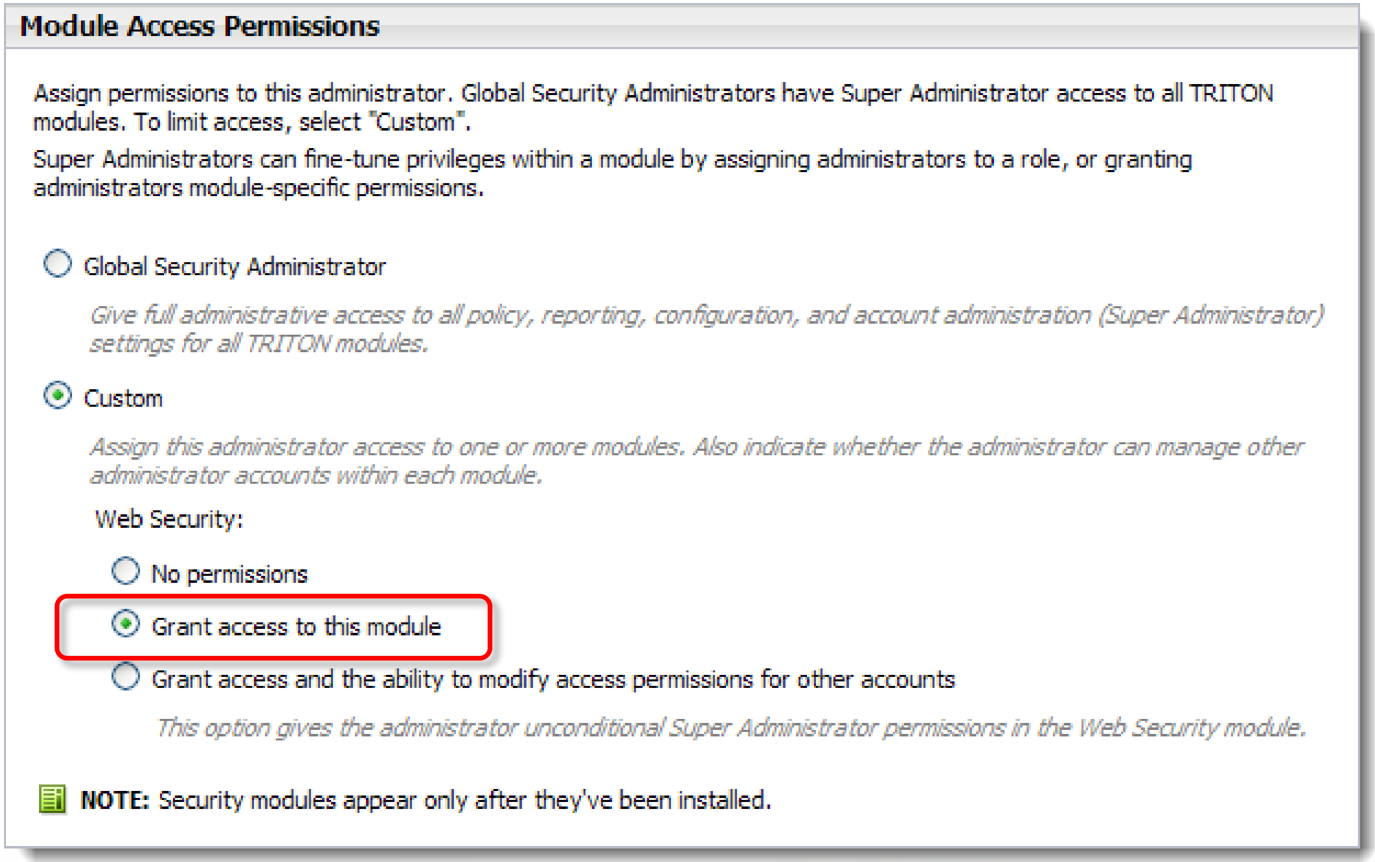
□	User Name	Type	Email Address	Permissions
□	admin	Local	admin@mydomain.com	Global Security Administrator
□	auditor	Local	auditor@mydomian.com	Web Security (access only)
□	Websense	Network	Websense@testadw2k3.techsupport2k3.com	Web Security (access and account management)

Administrator Access Permissions

- Defining TRITON - Web Security account access:
  - **Grant access to this module**
    - Provides basic access to TRITON - Web Security.
    - Until the account is assigned to a role and granted delegated administrator permissions, it can only view the Web Security Today page.
    - You can limit this account type to a single role.
  - **Grant access and the ability to modify access permissions for other accounts**
    - Defines an unconditional Super Administrator account.
    - Gives full access to all TRITON - Web Security features and functions.
    - This account type can access, view, and modify any role.

Administrator Access Permissions

- Defining TRITON - Web Security account access:
  - Grant access to this module
    - Select this option when creating delegated administrators.



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

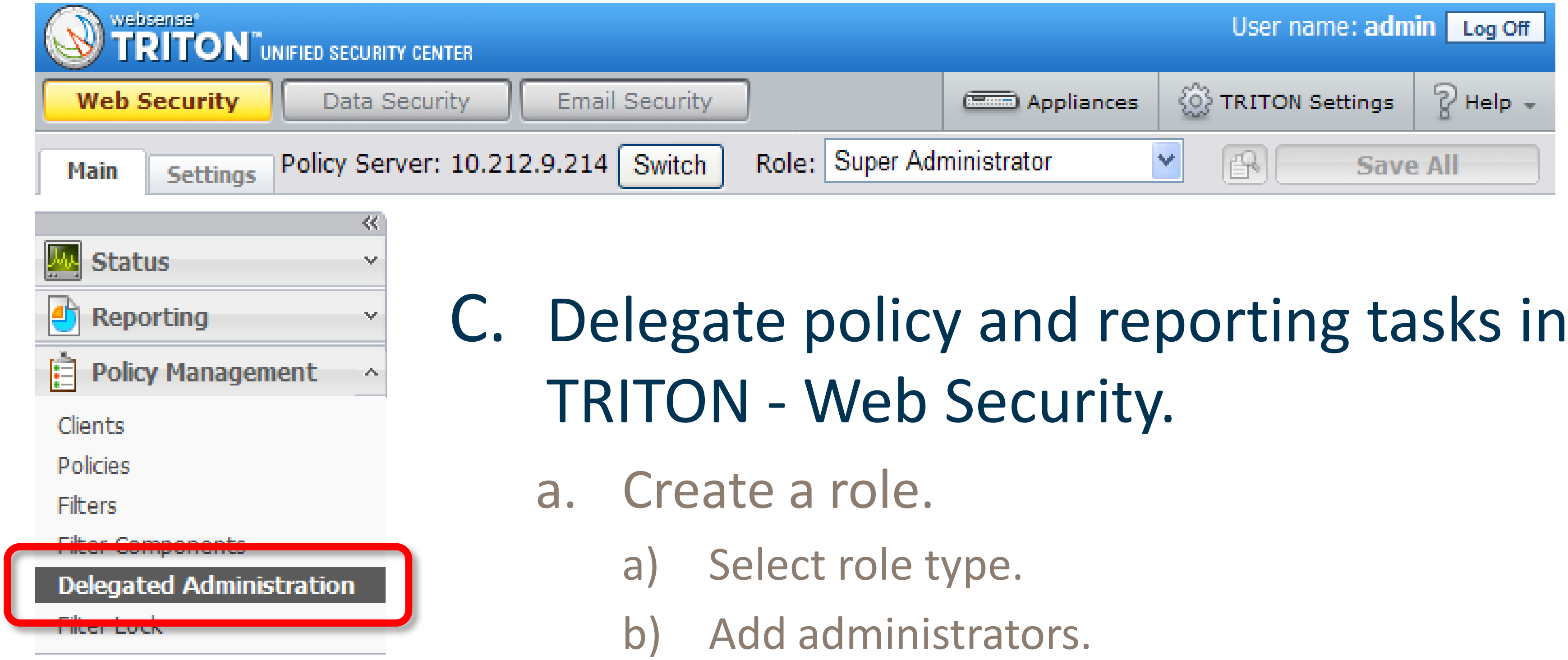
● Grant access to this module

○ 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.

Implementation – Phase Three



User name: admin

Policy Server: 10.212.9.214

Role: Super Administrator

C. Delegate policy and reporting tasks in TRITON - Web Security.

   a. Create a role.

      a) Select role type.

      b) Add administrators.

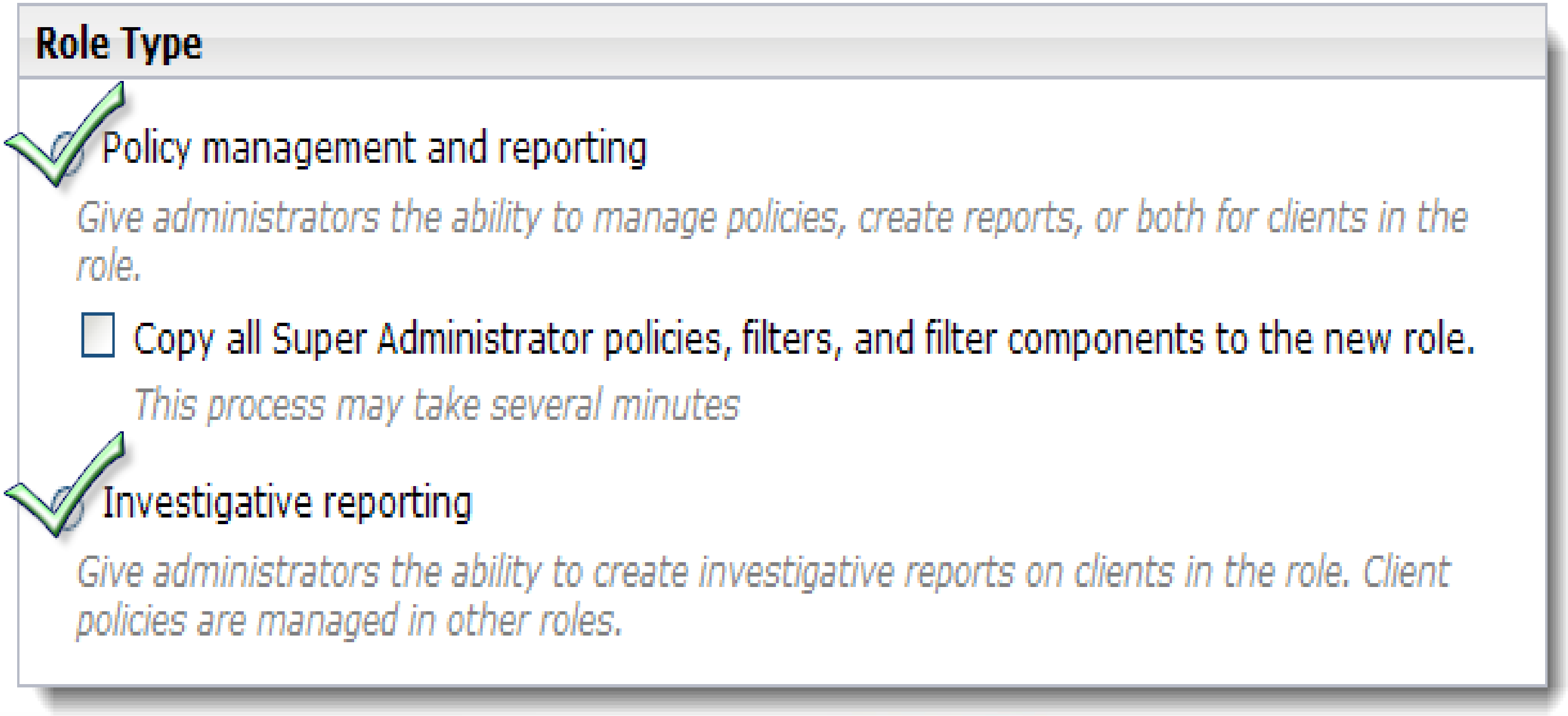
      c) Add managed clients.

      d) Define reporting permissions.

   b. Ensure new administrators know how to perform their tasks.

Creating Roles

- Delegated administration roles consist of related clients and the administrators who manage their policies, run reports on Internet usage, or both.
  - There are 2 role types:



Role Type

✓ Policy management and reporting

Give administrators the ability to manage policies, create reports, or both for clients in the role.

□ Copy all Super Administrator policies, filters, and filter components to the new role.

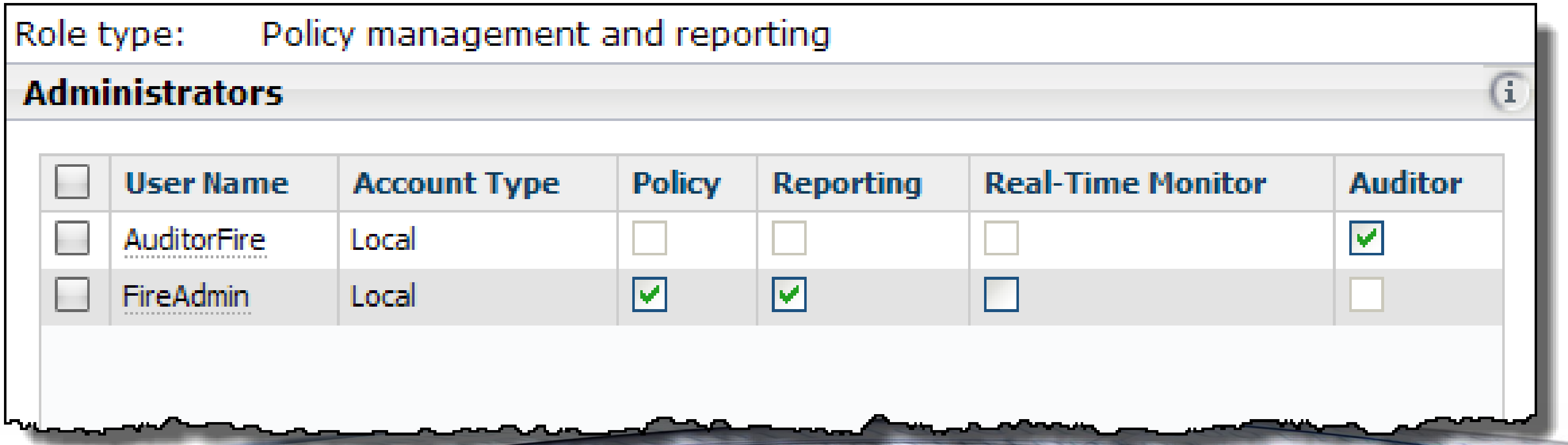
This process may take several minutes

✓ Investigative reporting

Give administrators the ability to create investigative reports on clients in the role. Client policies are managed in other roles.

Roles 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.
  - Only the *Default category* and *Default protocol* filters are copied from the Super Administrator’s role.
  - Check box option allows copying all policies, etc.
  - Clients can exist in only **one** policy management role.



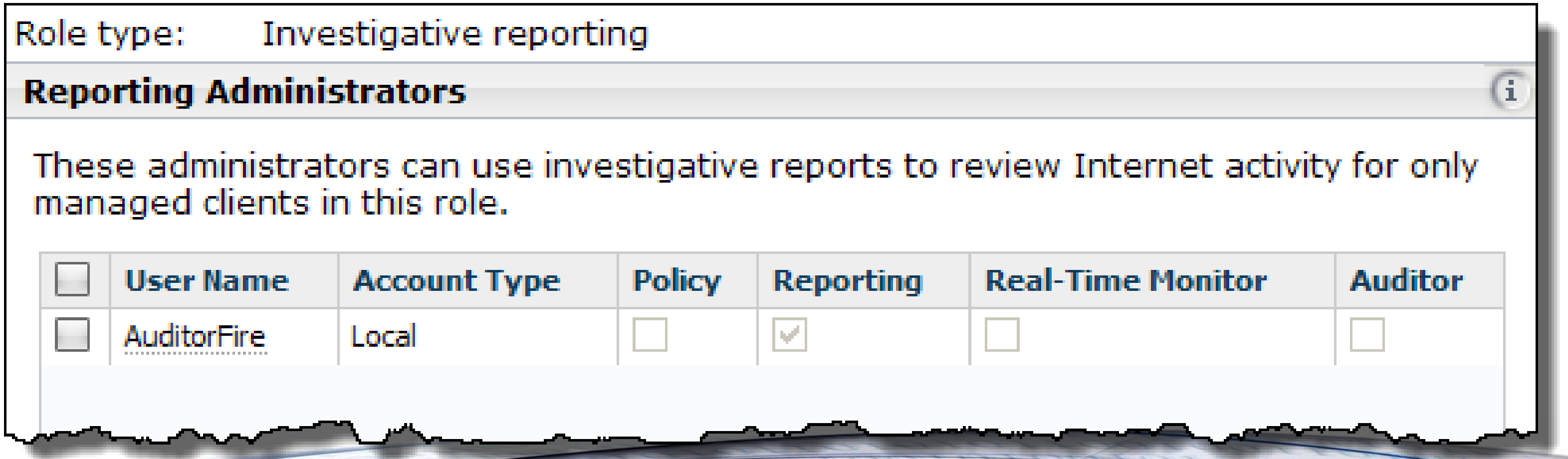
Role type: Policy management and reporting

Administrators

□	User Name	Account Type	Policy	Reporting	Real-Time Monitor	Auditor
□	AuditorFire	Local	□	□	□	☑
□	FireAdmin	Local	☑	☑	□	□

Roles Types

- **Investigative reporting**
  - Limits administrators to report only on their managed clients.
  - Client policies are managed in other roles.
  - Client can be in **multiple** investigative reporting roles.
  - Caution! Reporting permissions are cumulative.
  - Policy, Real-Time Monitor, and Auditor permissions are not available.



Role type: Investigative reporting

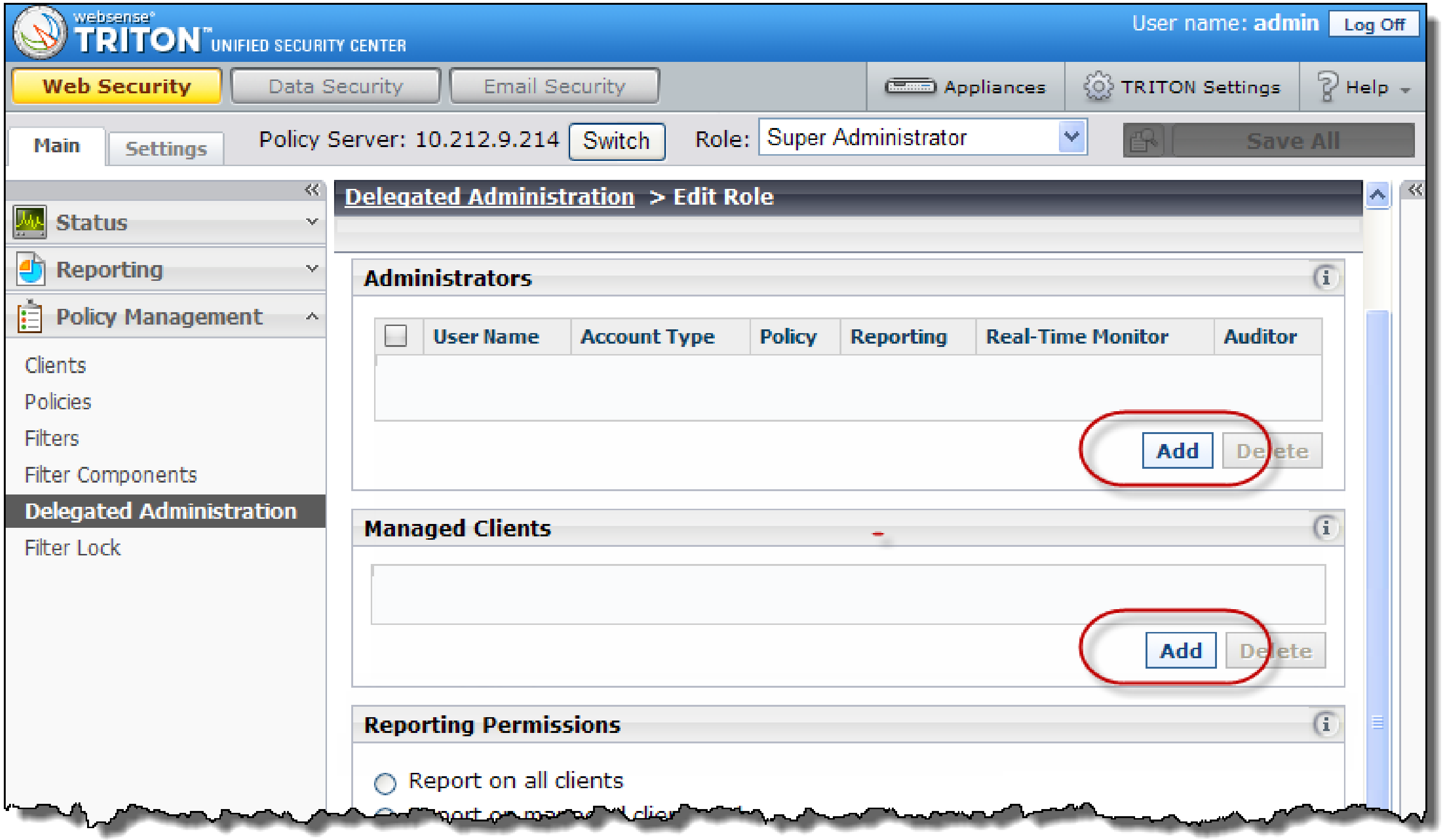
Reporting Administrators

These administrators can use investigative reports to review Internet activity for only managed clients in this role.

□	User Name	Account Type	Policy	Reporting	Real-Time Monitor	Auditor
□	AuditorFire	Local	□	☑	□	□

Add Administrator & Clients

- Add delegated administrator responsible for the role.
- Add the managed clients.

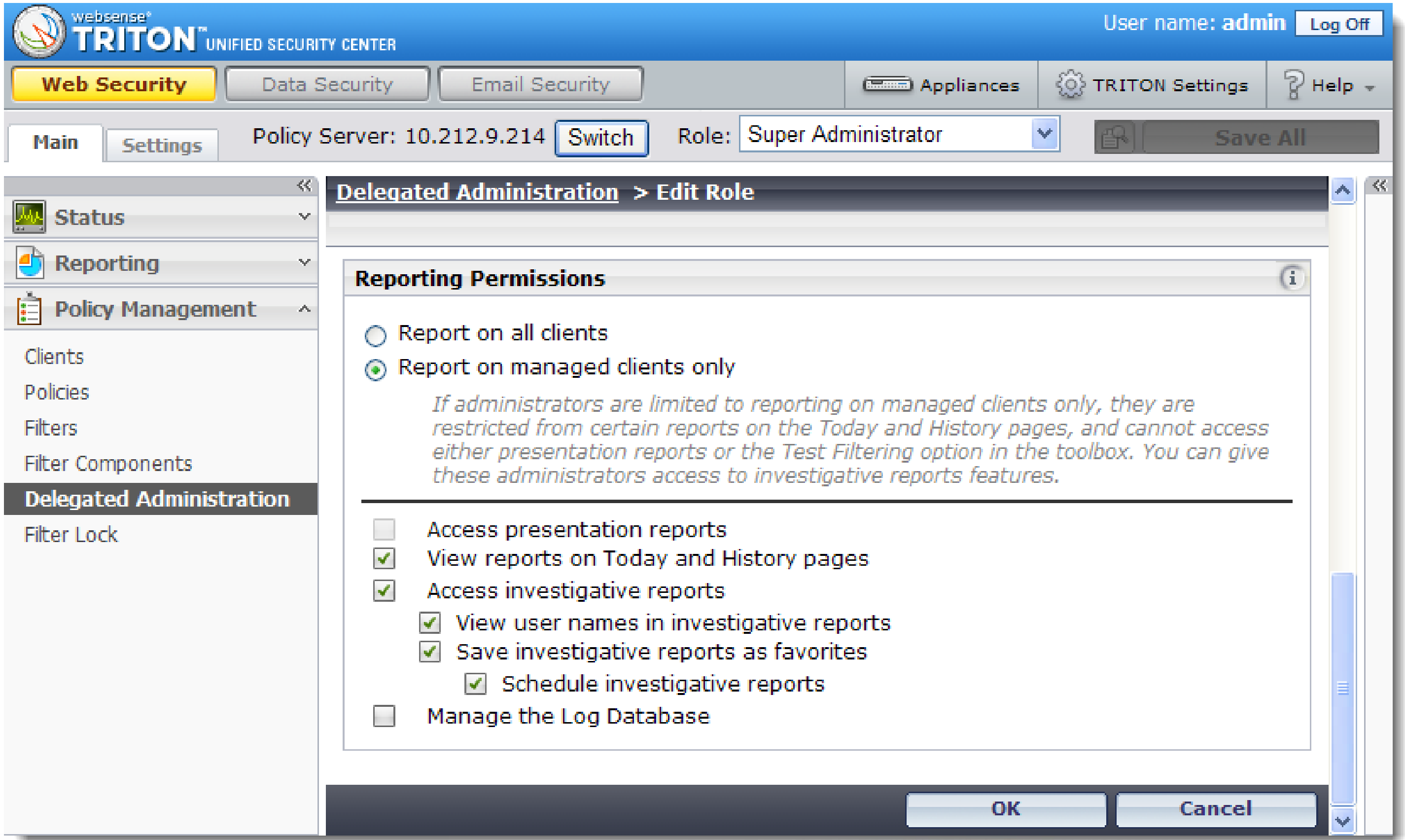


□	User Name	Account Type	Policy	Reporting	Real-Time Monitor	Auditor

○ Report on all clients

Set Reporting Permissions

- Select the *report on managed clients only* option to define specific managed clients.
  - **TIP:** Limit access to the Log Database.



Policy Server: 10.212.9.214

Role: Super Administrator

Delegated Administration > Edit Role

Reporting Permissions

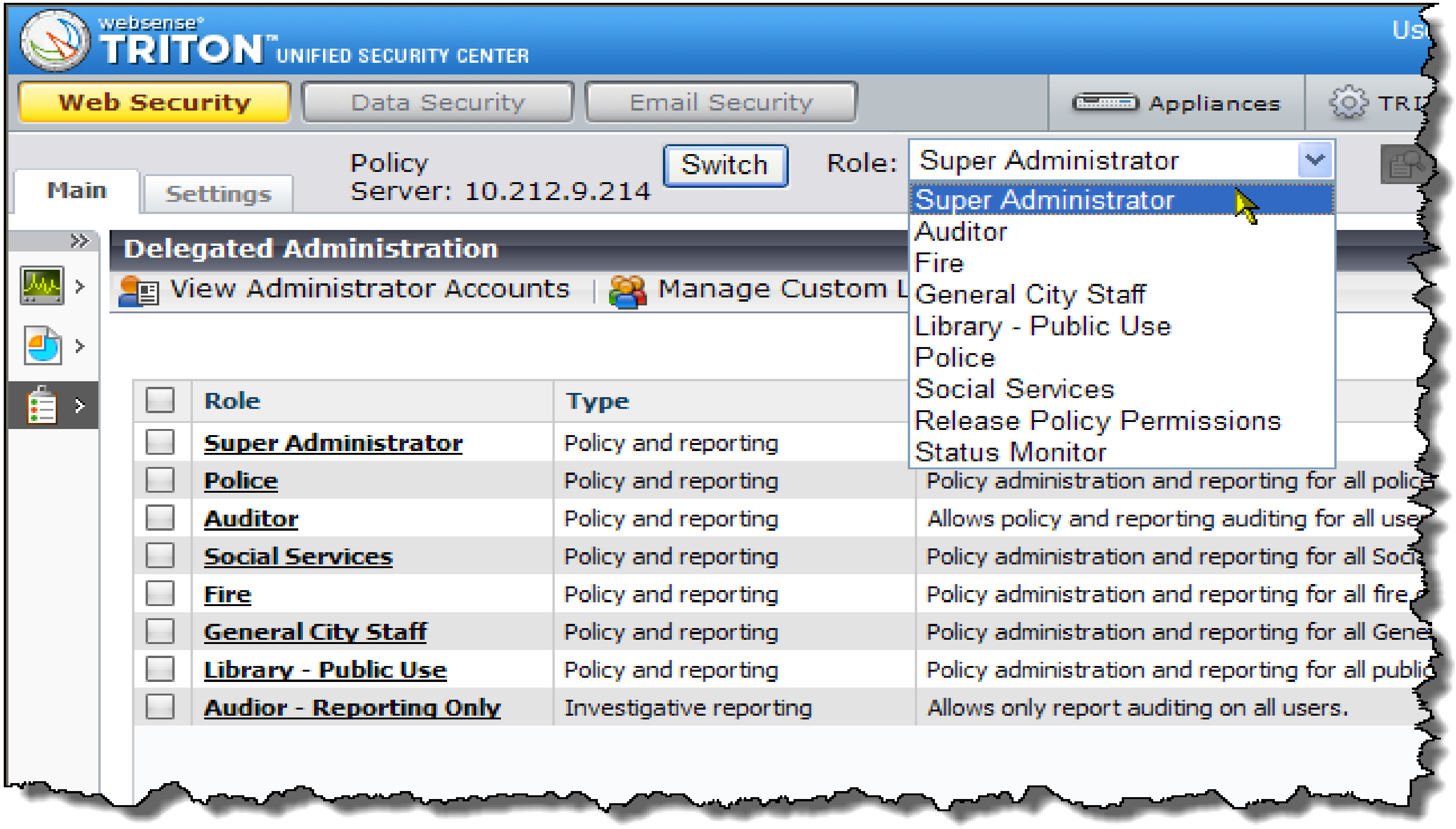
○ Report on all clients
● Report on managed clients only

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

Navigating Between Roles

- You must re-login into TRITON to see new roles.



Role: Super Administrator

- Super Administrator
- Auditor
- Fire
- General City Staff
- Library - Public Use
- Police
- Social Services
- Release Policy Permissions
- Status Monitor

□	Role	Type	
□	Super Administrator	Policy and reporting	
□	Police	Policy and reporting	Policy administration and reporting for all police
□	Auditor	Policy and reporting	Allows policy and reporting auditing for all use
□	Social Services	Policy and reporting	Policy administration and reporting for all Soci
□	Fire	Policy and reporting	Policy administration and reporting for all fire
□	General City Staff	Policy and reporting	Policy administration and reporting for all Gene
□	Library - Public Use	Policy and reporting	Policy administration and reporting for all publi
□	Audior - Reporting Only	Investigative reporting	Allows only report auditing on all users.

Train New Administrators

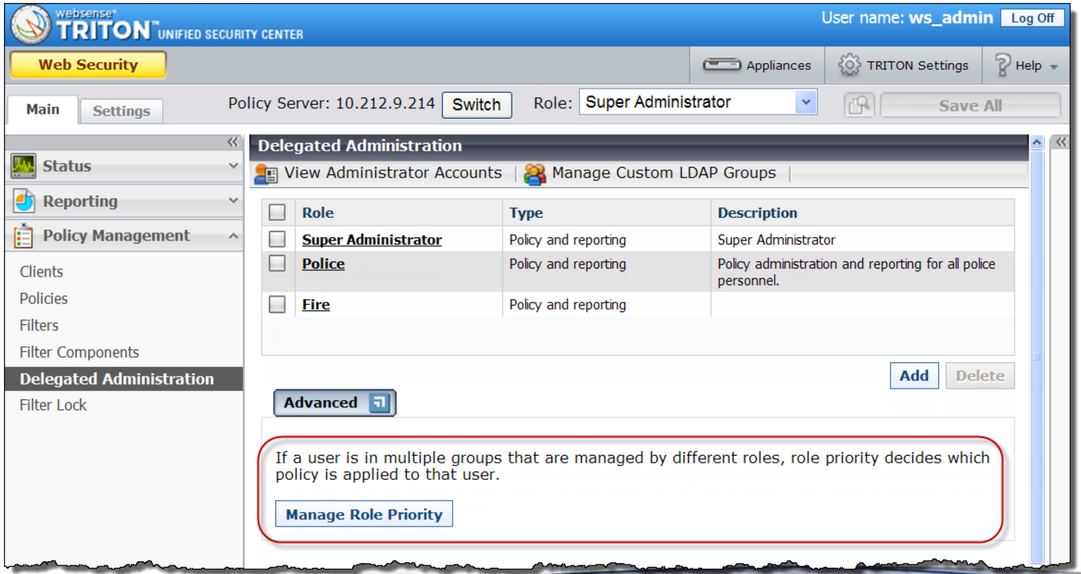
- New administrators need to understand how to:
  - Access TRITON - Web Security
  - Select appropriate role
  - Select the appropriate Policy Server
  - Create filters and policies
  - Add managed clients and assign policies
  - Access reporting tools
- New User Orientation
  - Select ‘New User Orientation’ available in Help for TRITON - Web Security.
  - Jump Start Webinars series.

Implementation Recap

- The three implementation phases:
  - Prepare the Websense Web Security environment.
  - Set up administrator accounts via TRITON Settings.
  - Delegate policy and reporting tasks in TRITON - Web Security.
- Demonstration
  - "Let's implement a delegated administration role from start to finish."

Filtering Precedence

- A single user may exist in groups, managed by different delegated administration roles.
- Manage Role Priority allows setting role precedence.
  - Use **Manage Role Priority** to tell Websense what to do if different policies apply to the same user due to overlap.
  - Setting is only available in the Super Administrator role.



Policy Server: 10.212.9.214

Role: Super Administrator

Delegated Administration

□	Role	Type	Description
□	Super Administrator	Policy and reporting	Super Administrator
□	Police	Policy and reporting	Policy administration and reporting for all police personnel.
□	Fire	Policy and reporting	

If a user is in multiple groups that are managed by different roles, role priority decides which policy is applied to that user.

Filtering Precedence

- Clients NOT identified in specific a delegated role are filtered by the Super Administrator’s role.
- Conversely, clients identified in a specific delegated role are NOT filtered by the Super Administrator’s role.
- When a client is identified both roles:
  - Delegated role takes precedence when:
    - Delegated role contains a client ***user*** directory object.
    - Super Administrator role contains a ***group*** directory object.
  - Super Administrator role takes precedence when:
    - Super Administrator role contains a client ***user*** directory object.
    - Delegated role contains a ***group*** directory object.

Filtering Order

- Determine which policy applies, in this order:
  1. Policy assigned to the user.
  2. Policy assigned to the IP address (computer or network) of the machine being used.
  3. Policies assigned to groups the user belongs to.
  4. Policies assigned to the user’s domain (OU).
  5. The Default policy in the Super Administrator’s role.
- The first applicable policy found is used.
- When multiple roles exist, filtering order still applies.
- TRITON - Web Security Help

Compliance

- Ensure filtering control is handled responsibly and in accordance with your organization's acceptable use policies:
  - Use Reports to Evaluate Filtering
  - Review the Audit Log page
  - Use the Auditor account
    - Views policy and configuration settings only.
- Demonstration
  - "Let's also allow the auditor to view reports."
    - Non-documented tip.
  - Reporting permissions are cumulative.
    - If reporting is permitted for an administrator in one role, then that administrator will have reporting privileges available in all roles.

Implementation

- Prepare the Websense Web Security environment.
  1. Configure directory service for TRITON - Web Security. (optional)
  2. Establish baseline filtering.
  3. Create category and protocol filtering restrictions.
- Set up administrator accounts via TRITON Settings.
  1. Configure directory service for adding administrators. (optional)
  2. Configure email settings for administrators.
  3. Grant administrators access permissions.
- Delegate policy and reporting tasks in TRITON - Web Security.
  1. Create a role.
     a. Select role type.
     b. Add administrators to the role.
     c. Add clients to the role.
     d. Define reporting permissions.
  2. Ensure new administrators know how to perform their tasks.

Additional Resources

- Delegated Administration Quick Start
- TRITON - Web Security Help tutorial (page 285)
- Upgrading User Quick Start Tutorial (page 36)
- Troubleshooting Delegated Administration logon issues in TRITON - Web Security
- Cannot log into TRITON Unified Security Center with Websense Administrator account after upgrading to v7.6
- How do I configure Logon Directory settings?
- Delegated Administrator cannot log in after upgrading to v7.6
- How to Reset the Admin password for TRITON

Support Online Resources

websense ESSENTIAL INFORMATION PROTECTION™

Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.

Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.

Tech Alerts

- Subscribe to receive product-specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

ask.websense.com

- Create and manage support service requests using our online portal.

Webinar Announcement

Webinar

Update

Title: **User and group based reporting in TRITON - Web Security: Best practices and troubleshooting**

Date: **March 14, 2012**

Time: **8:00 A.M. PDT (GMT -8)**

How to register: http://www.websense.com/content/ SupportWebinars.aspx

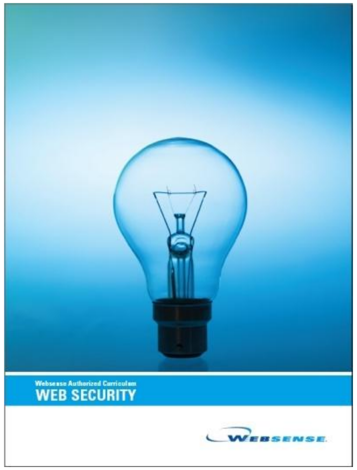
Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit: http://www.websense.com/findaclass
- Websense Training Partners also offer classes online and onsite at your location.
- For more information, please send email to:

readiness@websense.com

WEBSENSE® Authorized Training Partner

WEBSENSE® Certified Instructor



Websense Authorized Curriculum
WEB SECURITY
WEBSENSE