CHAPTER 6

Administering Trend Micro InterScan for Cisco CSC SSM

This chapter describes administration tasks, and includes the following sections:

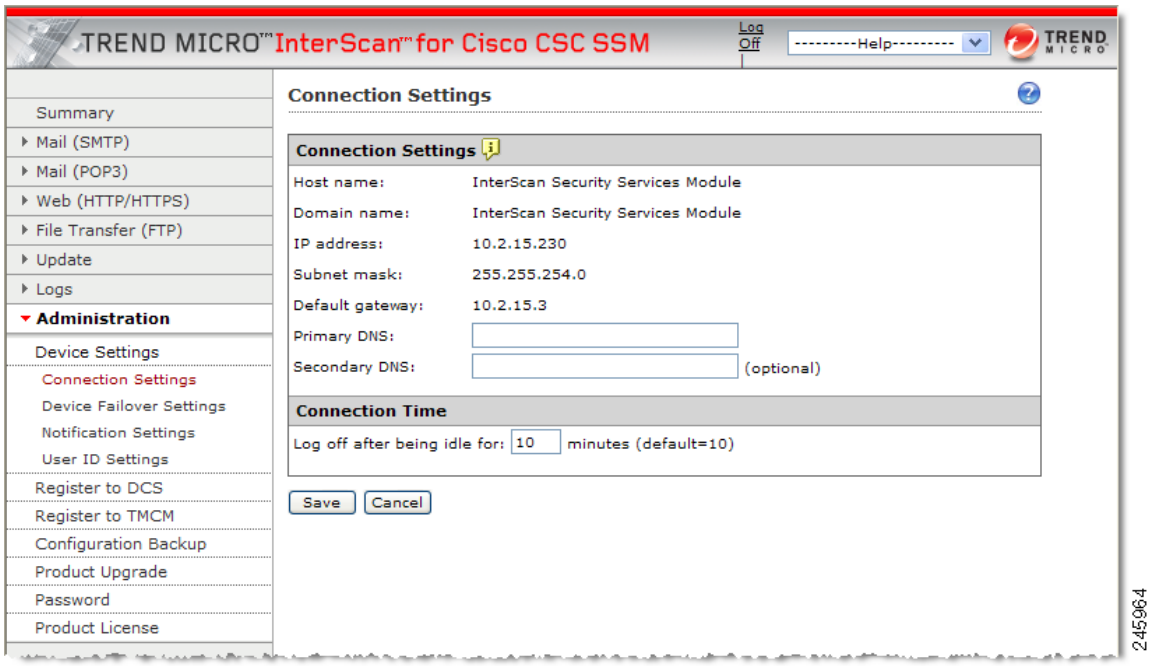
Configuring Connection Settings

To configure connection settings, perform the following steps:

Step 1 To view current network connection settings, choose **Administration > Device Settings > Connection Settings**.

The Connection Settings window (shown in Figure 6-1) displays selections that you made during installation.

Figure 6-1 Connection Settings Window



You can change the Primary DNS and Secondary DNS IP address fields in this window.

Step 2 To change other connection settings, in the ASDM, such as hostname, domain name, or IP address, choose **Configuration > Trend Micro Content Security** and from the menu, choose **CSC Setup**.

Step 3 You can also change these settings using the CLI. Log in to the CLI, and enter the **session 1** command. If this is the first time you have logged in to the CLI, use the default username (cisco) and password (cisco). You are prompted to change your password.

Step 4 Choose option **1**, **Network Settings**, from the Trend Micro InterScan for Cisco CSC SSM Setup Wizard menu.

Step 5 Follow the on-screen instructions to change the settings.

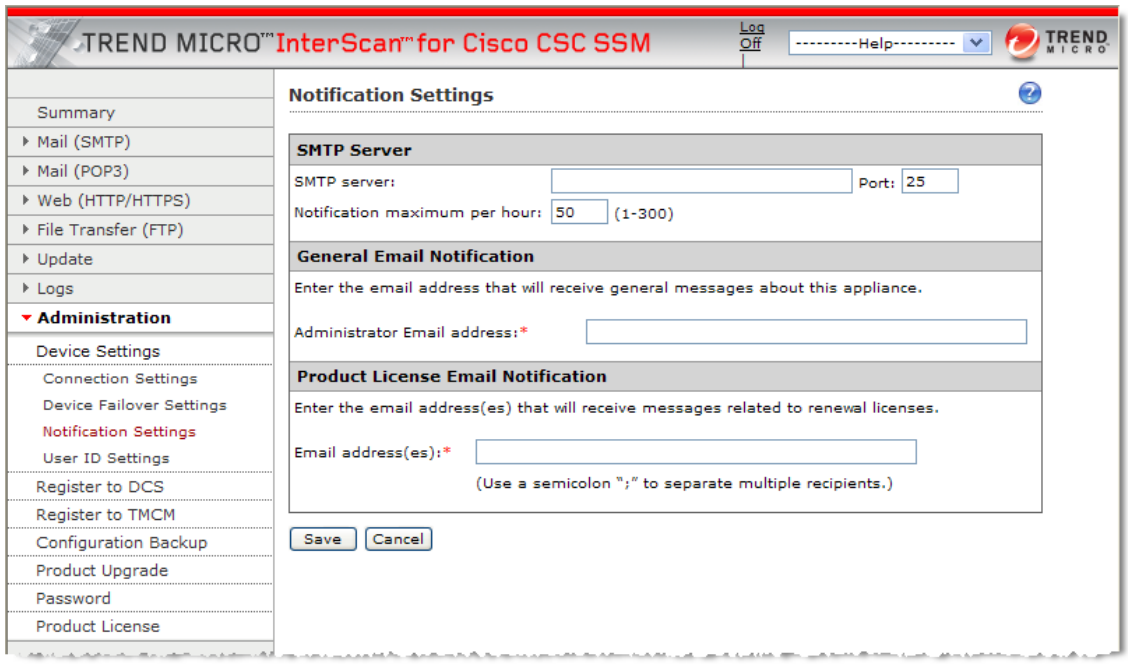
For more information, see the "Reimaging the CSC SSM" section on page B-5.

Managing Administrator E-mail and Notification Settings

The Notification Settings window (shown in Figure 6-2) allows you to do the following:

- View or change the administrator e-mail address that you chose on the Host Configuration window during installation.
- View the SMTP server IP address and port you chose during installation on the Host Configuration window.
- Configure the maximum number of administrator notifications per hour.

Figure 6-2 Notification Settings Window



To make changes on the Notification Settings window, perform the following steps:

Step 1 Enter the new information and click **Save**.

Step 2 You can also make these changes in ASDM. Choose **Configuration > Trend Micro Content Security** and from the menu, choose **CSC Setup**.

Note For more information about the Register to DCS and Register to TMCM menu items, see the "Using CSC SSM with Trend Micro Damage Cleanup Services" section on page D-1 and the "Using CSC SSM with Trend Micro Control Manager" section on page C-1.

Configuring User ID Settings

The user identification settings allow you to identify individual users and groups in your organization making HTTP/HTTPS connections through the CSC SSM. The domain user's identification allows you to:

- Identify the user roles
- Create URL filtering and blocking policies that are user- or group-specific

The Trend Micro Domain Controller Agent offers transparent user identification for users in a Windows-based directory service. The Domain Controller Agent communicates with the Domain Controller to gather up-to-date user login information and provide it to the CSC SSM. This information can be used to create URL filtering and blocking policies applied to specific users and groups.

Note User classification cannot separate users that share an IP address. When users have the same IP address, user classification is not supported.

Also, user classification cannot acquire user information if a NAT or downstream proxy exists because the CSC SSM cannot get the actual client IP address to map to the correct user.

The User Identification page includes the following information:

- Selecting the User Identification Method, page 6-4
- Configuring the Cache Time Limitations, page 6-5
- About the Domain Controller Agent, page 6-6
- Adding Domain Controller Server Credentials, page 6-11

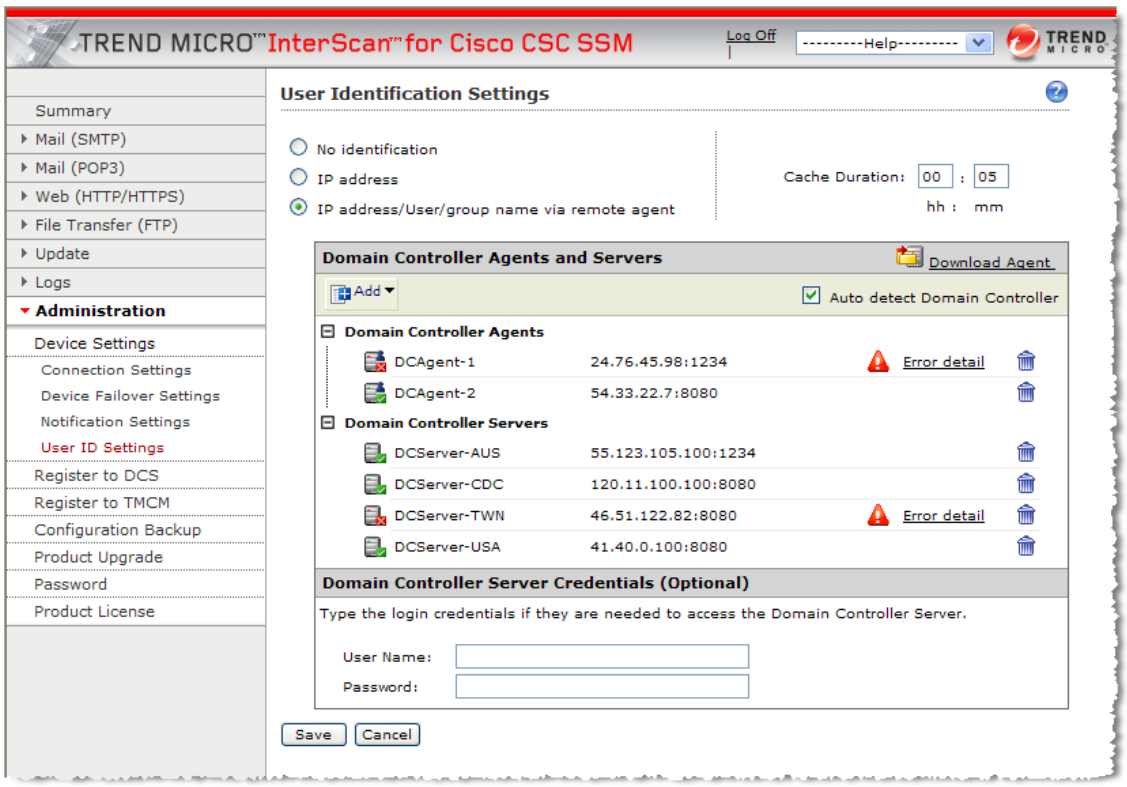
Selecting the User Identification Method

You can identify users through IP addresses or by user/group names via proxy authorization, as shown in Figure 6-3.

Identifying users enables you to do the following:

- Set up user and group policies for URL filtering and blocking
- Display user information in the violation logs
- Have domain name and account information appear in the HTTP debugging log

Figure 6-3 User Identification Settings



To configure the user identification settings, perform the following steps:

Step 1 Choose **Administration > Device Settings > User ID Settings**.

Step 2 Click one of the following radio buttons:

- No identification—No user or group identification is used for the connection and the global user policy applies.
- IP address—Users will be identified by an IP address.
- IP address/User/group name via remote agent—Using this setting allows you to identify both individual users and groups, by name (first) or IP address (second). This setting requires configuration of the Domain Controller Agent and Domain Controller Server.

Step 3 Perform the steps in the cache time limitation procedure listed in the "Configuring the Cache Time Limitations" section on page 6-5.

Configuring the Cache Time Limitations

The cache settings pertain to the amount of time that the IP address remains associated with a user without reverification. The time value you set for caching specifies how often the Domain Controller Agent should verify that a particular IP address is still associated with a specific user.

Note Cache configuration is only necessary if you choose **IP address/User/group name via remote agent** as the method of user identification.

To identify the cache duration, perform the following steps:

Step 1 Enter the hours and minutes values to define the length of time that cached information will associate an IP address with a specific user. By default, the client IP address is reverified every 15 minutes.

```
Example:
    Cache duration: 24: (hh) 00: (mm)
```

Step 2 Install the Domain Controller Agent, as shown in the "Installing the Domain Controller Agent" section on page 6-7.

About the Domain Controller Agent

The Trend Micro Domain Controller Agent queries each domain controller for user login sessions every seven seconds by default, obtaining the user name and workstation name for each login session. For each login session identified, the Domain Controller Agent performs a DNS lookup to resolve the workstation name to an IP address, and records the resulting user name/IP address pair.

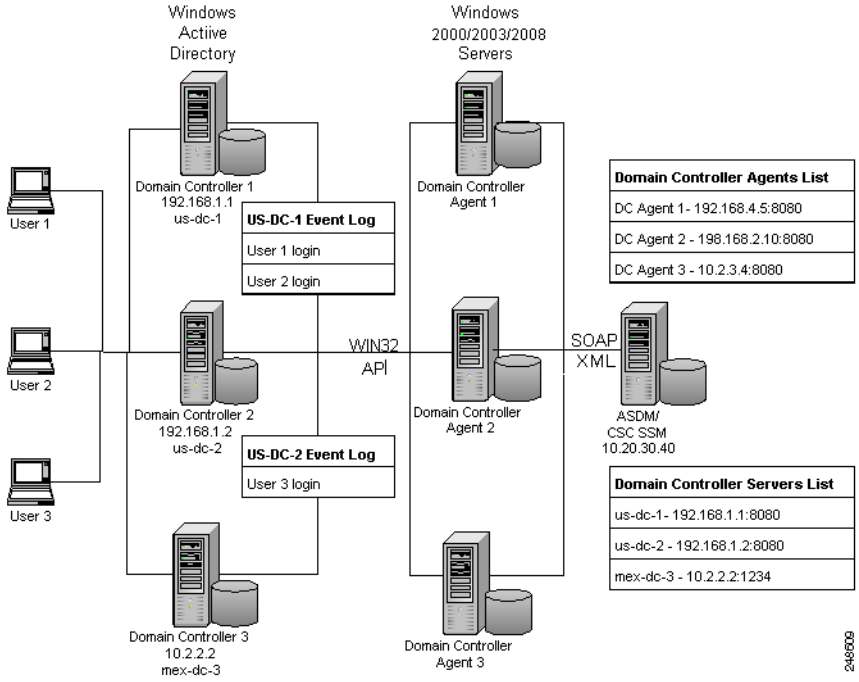
The Domain Controller Agent uses the Win32 API to communicate with the Domain Controller Server and SOAP/XML to transmit login data to the CSC SSM. The user data that the Domain Controller Agent sends to the software components equals about 80 bytes per user name/IP address pair. On average, the Domain Controller Agent uses 8-10 MB of RAM, but this varies according to the number of login sessions per network Domain Controller.

The CSC SSM supports up to 32 Domain Controllers, and up to eight Domain Controller Agents can be assigned to the CSC SSM. Having multiple agents provides redundancy. If one agent goes down, another agent will act as backup. Although eight Domain Controller Agents can be assigned to the CSC SSM, only two or three would be necessary in most network configurations.

Note The Domain Controller Agent file (IdAgentInst.msi) may be updated periodically during maintenance releases. You will need to uninstall the old file and install the updated file to take advantage of any updates to the Domain Controller Agent functions.

To uninstall the Domain Controller Agent, perform the following steps:
1. Choose **Settings > Control Panel > Add or Remove Programs**.
2. Select **Trend Micro IdAgent**.
3. Click **Remove**.

Figure 6-4 Network Configuration for Domain Controller Agent Installation



Installing the Domain Controller Agent

Trend Micro recommends that the Domain Controller Agent be installed on the same server as the Domain Controller.

The Domain Controller Agent may be installed on the following Windows operating systems: (XP, 2000 Server/Professional, 2003, or 2008) or on the Active Directory Server, if needed. For more information about adding Domain Controller servers manually, see the "Adding a Domain Controller Agent or Server to CSC SSM" section on page 6-8.

After installation, Domain Controller Agents will poll Domain Controllers every seven seconds for new login information. The login information is then used to configure and enforce URL filtering and blocking policies for users and groups.

To install the Domain Controller Agent, perform the following steps:

Step 1 Before installation, verify that logging is enabled for logon events. If it is not, the Domain Controller Agent cannot access user information from the Domain Controller logs.

a. To enable 672/673 (or 4768/4769 for Windows 2008) logon events in the Domain Controller event log, choose **Start > Administrative Tools > Domain Controller Security Policy** on each Domain Controller machine.

b. Choose **Security Settings > Local Policies > Audit Policy**.

c. Define the policy setting for the Audit Account login events policy (audit success).

Step 2 Log in with Domain Admins privileges (and administrator privileges) to the server (Windows 2000, 2003, or 2008) on which the Domain Controller Agent will be installed.

Step 3 Access the CSC SSM UI at: http://<CSC SSM IP address:port_number> and log in.

Step 4 Choose **Administration > Device Settings > User ID Settings**.

Step 5 Click the **Download Agent** link and follow the on-screen instructions.

a. Click **Run** or **Save**.

Note This operation is fully supported in Internet Explorer™ 6.0 or later. If you are using Mozilla Firefox™, you can only save, not run, the installation.

- If you choose Run, the agent installation will be saved to a temp folder and launched.
- If you choose Save, you will need to launch it later manually.

Note To launch the agent installer later, browse to the folder in which it was saved and double-click the IdAgentInst.msi file.

b. In the Setup Wizard, click **Next**.

c. Check the license agreement check box and click **Next**.

d. Click **Next** in the Destination folder screen.

Note The destination folder cannot be changed. The installer auto-detects the appropriate system drive.

e. Click **Install**. A progress bar displays.

f. Click **Finish** when the setup is complete.

Step 6 Repeat Step 1 through Step 5 for additional installations of Domain Controller Agents. A maximum of eight Domain Controller Agents can point to one CSC SSM.

Step 7 Add the Domain Controller Agent and Domain Controller to the CSC SSM according to the procedure listed in the "Adding a Domain Controller Agent or Server to CSC SSM" section on page 6-8.

Step 8 Add the Domain Controller login credentials according to the procedure listed in the "Adding Domain Controller Server Credentials" section on page 6-11.

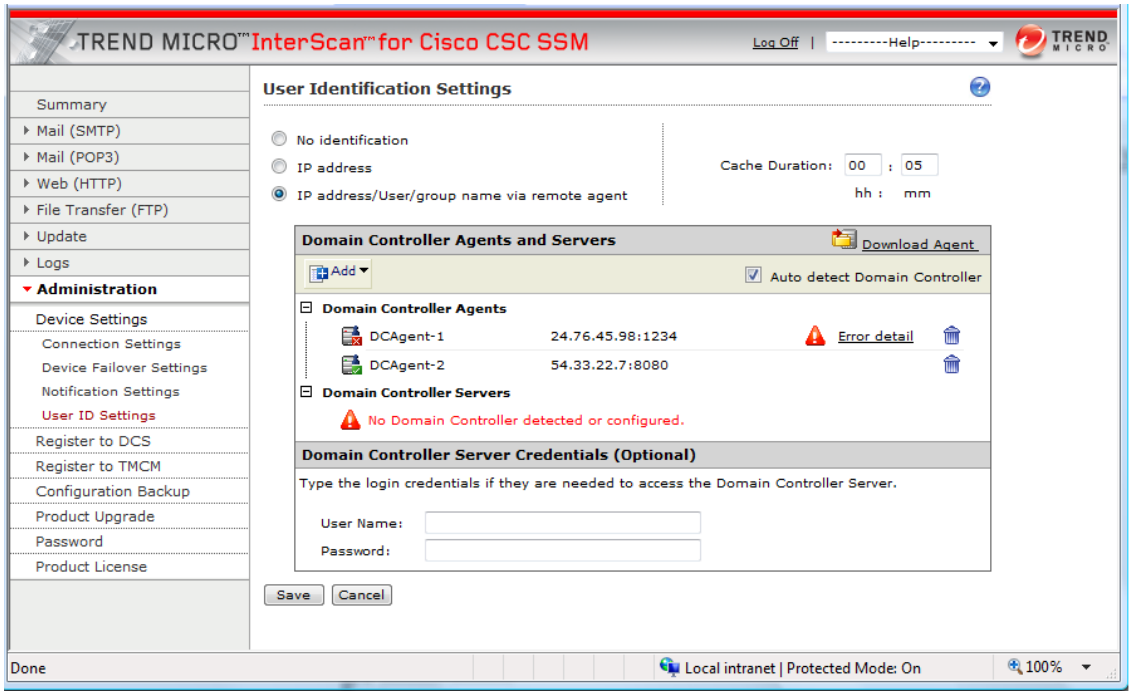
Adding a Domain Controller Agent or Server to CSC SSM

The CSC SSM requires that the Domain Controller Agents and Domain Controller Servers be added to the CSC SSM to permit URL filtering and blocking policies that are user or group specific.

- Adding Domain Controller Agents allows the CSC SSM to access user logon information from the Domain Controller Agent.
- Adding the Domain Controller Server provides information to the Domain Controller Agent, which accesses the Domain Controller login events to retrieve user information.

Domain Controller Agents must be added manually. Domain Controllers can be added manually or automatically detected. If the auto-detect feature is enabled, Domain Controller Servers may still be added manually.

Figure 6-5 No Domain Controller Servers Detected



Auto-Detecting a Domain Controller Server

To auto-detect a Domain Controller Server, perform the following steps:

Step 1 Check the **Auto detect Domain Controller servers** check box.

Step 2 Verify that the detected Domain Controller Servers appear in the Domain Controller Servers list.

Note The auto-detect feature is available for Domain Controller Agents installed on Windows 2000, 2003 and 2008 servers. All Windows Active Directory Domain Controller Servers will be auto-detected, unless the Domain Controller Agent cannot access the Active Directory General Catalog. If this occurs, use the procedure shown in the "Adding a Domain Controller Agent or Server Manually" section on page 6-9.

After configuring the Domain Controller Agent on CSC SSM, the same configuration will be automatically propagated to the failover CSC SSM device(s).

Adding a Domain Controller Agent or Server Manually

To manually add a Domain Controller Agent or Domain Controller Server, perform the following steps:

Step 1 Click the **Add** icon in the Domain Controller Agents and Servers section, shown in Figure 6-3.

Step 2 Click **Agent** or **Server**, depending on what you need to add.

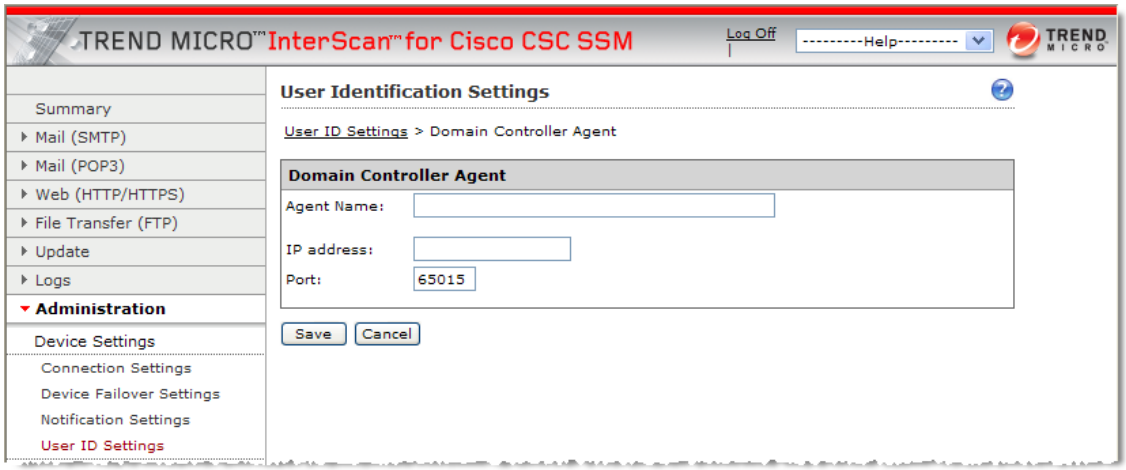
Step 3 For a Domain Controller Agent, type the following information:

- Host name or IP address—The hostname or IP address of the machine where the Domain Controller Agent is installed. (See Figure 6-6.)
- Port number—The port number of the machine on which the Domain Controller Agent is installed (The default port number 65015 is specified in the IdAgent.ini file ([Setting]/AgentPort parameter).

Step 4 Click **Save**.

The Domain Controller Agent name appears in the list shown in Figure 6-3.

Figure 6-6 Add a Domain Controller Agent



Step 5 For a Domain Controller Server, add the following information:

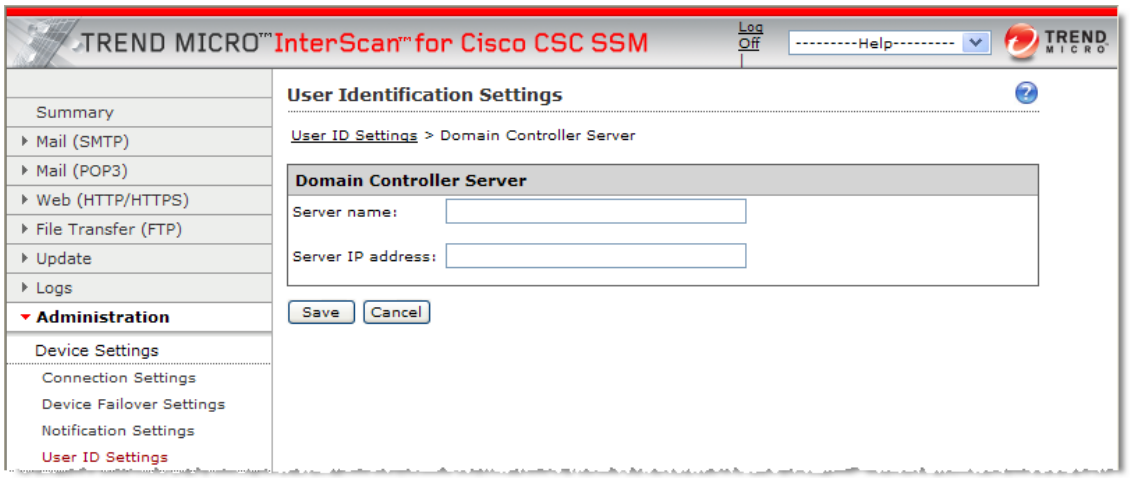
Note If the auto-detection method of adding Domain Controllers was used, do not add them manually.

- Agent Name—A descriptive name given to identify a specific Domain Controller Agent, not necessarily the machine name
- IP address—The IP address of the Domain Controller Server (See Figure 6-7.)

The Domain Controller Server name appears in the list shown in Figure 6-3.

Step 6 Click **Save**.

Figure 6-7 Add a Domain Controller Server



Step 7 To add Domain Controller Server credentials, see the "Adding Domain Controller Server Credentials" section on page 6-11.

After configuring the Domain Controller Agent on the CSC SSM, the same configuration will be automatically propagated to the failover CSC SSM device(s).

Deleting a Domain Controller Agent or Server

To remove a Domain Controller agent or server from the list, perform the following steps:

Step 1 Choose **Administration > Device Settings > User ID Settings**.

Step 2 Find the agent or server in the list.

Step 3 Click the trash can icon next to the name.

Step 4 Click **Save**.

Note To uninstall the Domain Controller Agent, go to the machine on which it was installed. Choose **Start > Settings > Control Panel > Add or Remove Programs**.

Adding Domain Controller Server Credentials

Adding Domain Controller Server credentials allows single sign-on, offering one-time authentication.

If the Domain Controller Agent is installed on a Windows machine, where the local system account does not have the permission to access the Domain Controller Server, the CSC SSM will not be able to query domain users and groups. To enable access, the CSC SSM user can enter the Domain Admins credentials in the username and password fields of the Domain Controller Server Credentials section of the screen shown in Figure 6-5.

Note It is important that all Domain Controller Servers share the same username and password credentials if the credentials are entered in this screen.

The Domain Controller Agent installation requires administrator privileges. If the Domain Controller Agent was installed by the domain administrator, then the agent service has domain administrator privileges. In that case, the user does not have to set the server credentials from the CSC SSM console.

To add Domain Controller Server credentials, perform the following steps:

Step 1 Choose **Administration > Device Settings > User ID Settings**.

Step 2 In the Domain Controller Server Credentials section at the bottom of the screen (see Figure 6-3), type the username in the domain name\username format.

Note The username added here must be a domain user with privileges to access the Domain Controller Server event log.

Step 3 Type the password.

Step 4 Click **Save**.

Backing Up Configuration Settings

This section describes how to back up configuration settings, and includes the following topics:

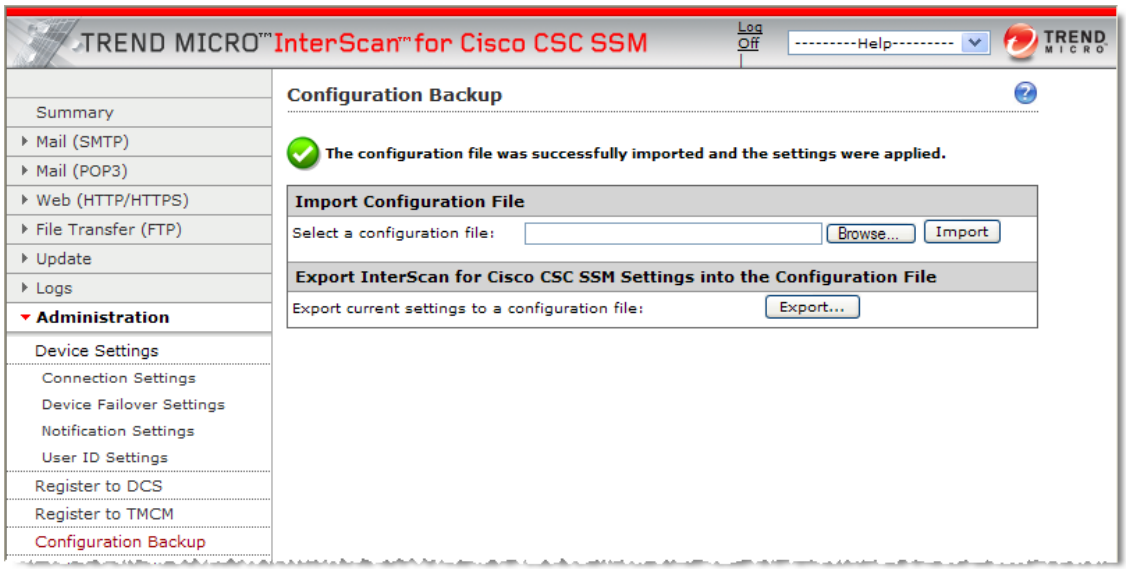
Trend Micro InterScan for Cisco CSC SSM provides the ability to back up your device configuration settings and save them in a compressed file. You can import the saved configuration settings and restore your system to those settings configured at the time they were saved.

Note A configuration backup is essential for recovery if you forget your ASDM or web GUI password, depending on how you have set your password-reset policy. For more information, see the "Recovering a Lost Password" section on page 8-5 and the "Modifying the Password-Reset Policy" section on page B-11.

As soon as you finish configuring Trend Micro InterScan for Cisco CSC SSM, create a configuration backup.

To back up configuration settings, choose **Administration > Configuration Backup** to display the Configuration Backup window, shown in Figure 6-8.

Figure 6-8 Configuration Backup Window with Successful Import Confirmation



Exporting a Configuration

To save configuration settings, perform the following steps:

Step 1 On the Configuration Backup window, click **Export**.

A File Download dialog box appears.

Step 2 Open the config.tgz, file, or save it to your computer.

Importing a Configuration

To restore configuration settings, perform the following steps:

Step 1 In the Configuration Backup window, click **Browse**.

Step 2 Locate the config.tgz file and click **Import**.

The filename appears in the Select a configuration file field. The saved configuration settings are restored to the adaptive security appliance.

Importing a saved configuration file restarts the scanning service, and the counters on the Summary window are reset.

Configuring Failover Settings

Trend Micro InterScan for Cisco CSC SSM enables you to replicate a configuration to a peer unit to support the device failover feature on the adaptive security appliance. Before you configure the peer device, or the CSC SSM on the failover device, finish configuring the primary device.

When you have fully configured the primary device, follow the steps exactly as described in Table 6-1 to configure the failover peer. Print a copy of the checklist that you can use to record your progress.

Table 6-1 Configuring Failover Settings Checklist

Step 1	Decide which appliance should act as the primary device, and which should act as the secondary device. Record the IP address of each device in the space provided: **IP Address(es):** _____ _____	❑ ❑
Step 2	Open a browser window and enter the following URL in the Address field: http://<primary device IP address>:8443. The Logon window appears. Log in, and choose **Administration > Device Settings > Device Failover Settings**.	❑
Step 3	Open a second browser window and enter the following URL in the Address field: http://<secondary device IP address>:8443. As in the Step 2, login, choose **Administration > Device Settings > Device Failover Settings**.	❑
Step 4	In the Device Failover Settings window for the primary device, enter the IP address of the secondary device in the Peer IP address field. Enter an encryption key of one to eight alphanumeric characters in the Encryption key field. Click **Save**, and then click **Enable**. The following message appears under the window title: `InterScan for CSC SSM could not establish a connection because the failover peer device is not yet configured. Please configure the failover peer device, then try again.` This message is normal behavior and appears because the peer is not yet configured.	❑

Step 5	In the Device Failover Settings window for the secondary device, enter the IP address of the primary device in the Peer IP address field. Enter the encryption key of one to eight alphanumeric characters in the Encryption key field. The encryption key must be identical to the key entered for the primary device. Click **Save**, and then click **Enable**. The following message appears under the window title:
	`InterScan for CSC SSM has successfully connected with the failover peer device.`
	`Do not click anything else at this time for the secondary device.`
		❑

Step 6	In the Device Failover Settings window for the primary device, click **Synchronize to peer**. The message in the Status field at the bottom of the windows should state the date and time of the synchronization, for example: `Status: Last synchronized with peer on: 04/29/2007 15:20:11`	❑

Caution Be sure you do not click **Synchronize to peer** at the end of Step 5, while you are still in the Device Failover Settings window for the secondary device. If you do, the configuration you have already set up on the primary device will be erased. You must perform manual synchronization from the primary device, as described in Step 6.

When you complete the steps on the checklist, the failover relationship has been successfully configured.

If you want to make a change to the configuration in the future, you should modify the configuration on the primary device only. Trend Micro InterScan for Cisco CSC SSM detects the configuration mismatch, and updates the peer with the configuration change you made on the first device.

The exception to the auto-synchronization feature is uploading a system patch. A patch must be applied on both the primary and secondary devices. For more information, see the "Installing Product Upgrades" section on page 6-15.

If the peer device becomes unavailable, an e-mail notification is sent to the administrator. The message continues to be sent periodically until the problem with the peer is resolved.

Installing Product Upgrades

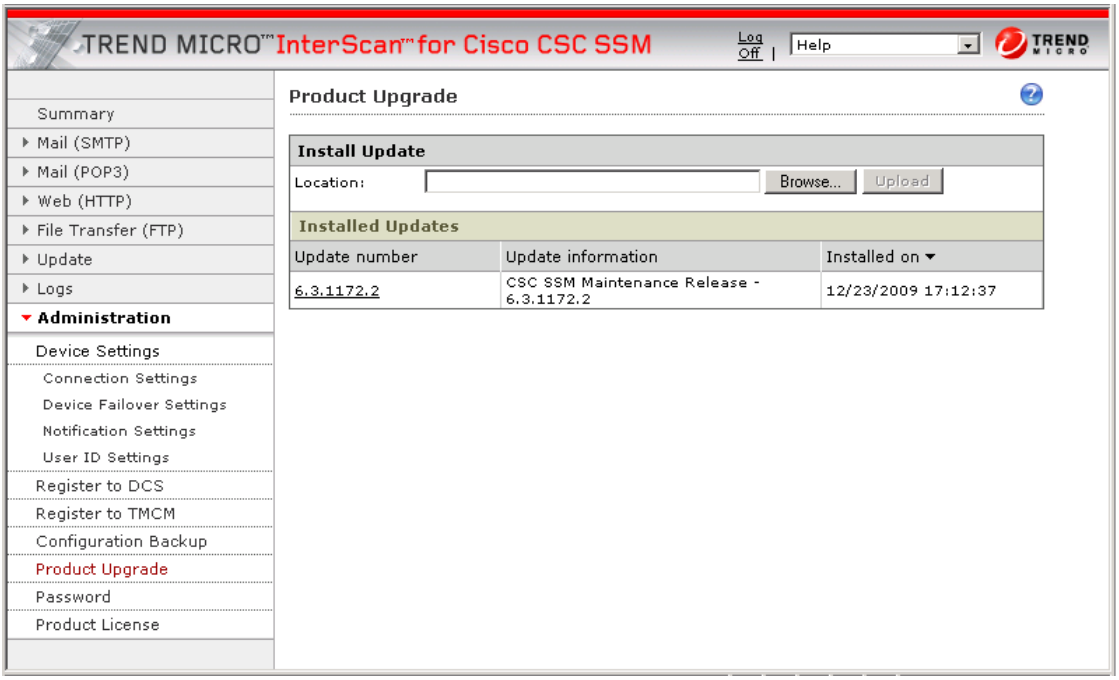
From time to time, a product upgrade becomes available that corrects a known issue or offers new functionality.

To install a product upgrade, perform the following steps:

Step 1 Download the system patch from the website or CD provided.

Step 2 Choose **Administration > Product Upgrade** to display the Upgrade window, shown in Figure 6-9.

Figure 6-9 Product Upgrade Window



Caution Upgrades may restart system services and interrupt system operation. Upgrading the system while the device is in operation may allow traffic containing viruses and malware through the network.

Step 3 Click **Browse** and locate the upgrade file.

Step 4 Click **Upload** to upload and install the upgrade.

The version number displays under the Update Number column if the upgrade is successful.

For information about installing and removing upgrades, see the online help for this window.

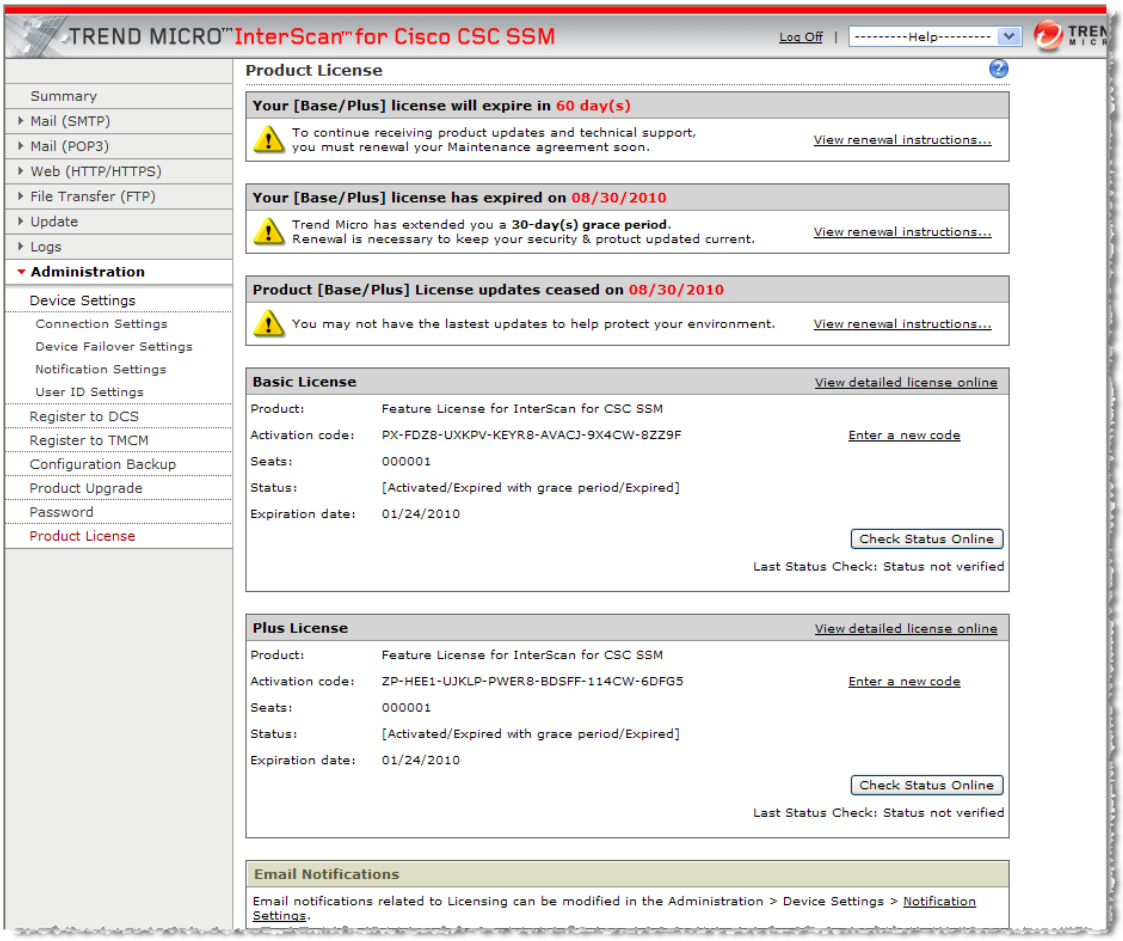
Viewing the Product License

This section describes product licensing information, and includes the following topics:

The Product License window (shown in Figure 6-10) allows you to view the status of your product license, which includes the following information:

- Activated license(s) (Basic License only, or Basic License and Plus License).
- License version, which should be Basic unless you are temporarily using an Evaluation copy.
- Activation code for your license.
- Number of licensed seats (users), which appears only for the Basic License, even if you have purchased the Plus License.
- License status, which should be “Activated.”
- License expiration date. If you have both the Basic and Plus Licenses, the expiration dates can be different.

Figure 6-10 Product License Window



If your license is not renewed, antivirus scanning continues with the version of the pattern file and scan engine that was valid at the time of expiration, plus a 30-day grace period. However, other features may become unavailable. For more information, see the "License Expiration" section on page 6-17.

License Expiration

As you approach and even pass your expiration dates, a message appears in the Summary window as well as the Product License window, similar to the example shown in Figure 6-11.

Figure 6-11 Product License Expiration Message

When your product license expires, you may continue using Trend Micro InterScan for Cisco CSC SSM, but you are no longer eligible to receive updates to the virus pattern file, scan engine, and other components. Your network may no longer be protected from new security threats.

If your Plus License expires, content filtering and URL filtering are no longer available. In this case, traffic is passed without filtering content or URLs.

If you purchased the Plus License after you purchased and installed the Basic License, the expiration dates are different. You can renew each license at different times as the renewal date approaches.

Licensing Information Links

To obtain licensing information, perform the following steps, or click the **View renewal instructions** link for basic or plus licenses:

Step 1 In the Product License window, click the **View detailed license online** link to access the online registration website, where you can view information about your license, and find renewal instructions.

Step 2 Click the **Check Status Online** button to display a message below the button that describes the status of your license, similar to the example shown in the previous figure.

For additional information, see the online help for the Product License window.

Note For information about product activation, see the *Cisco Security Appliance Configuration Guide using ASDM*.

Renewing a License

You can renew a license at any time after the product activation. Contact your reseller or Cisco about ordering a license renewal for the CSC SSM.

To renew a license for the CSC SSM, perform the following steps:

Step 1 Go to http://www.cisco.com/go/license/.

Step 2 Log in with your Cisco.com user ID, if necessary.

Step 3 Follow the on-screen instructions.

Step 4 Enter the renewal product code that you received when you registered the Product Authorization Key (PAK) that came with your Cisco Software License Certificate.

Step 5 Choose **Administration > Product License** after successfully renewing your license.

Step 6 Click **Check Status Online** to retrieve the latest license expiration date.

Notification Settings

You can enable or disable e-mail notifications as well as configure the e-mail notification schedule with optional warnings delivered at 60 and 30 days, or even one day before. These messages can continue up to 14 days after expiration.

You can also configure additional e-mail recipients (using a semicolon to separate multiple entries). You must enter the license renewal notification e-mail address, SMTP server IP address, and port, or the generated license renewal reminder e-mail cannot be delivered.

See the "Managing Administrator E-mail and Notification Settings" section on page 6-2 for more information about configuring the e-mail notification settings.

Note E-mail notification does not support the HTML format.