



CHAPTER 6

Administering Trend Micro InterScan for Cisco CSC SSM

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

- [Configuring Connection Settings, page 6-1](#)
- [Managing Administrator E-mail and Notification Settings, page 6-2](#)
- [Backing Up Configuration Settings, page 6-3](#)
- [Configuring Failover Settings, page 6-5](#)
- [Installing Product Upgrades, page 6-6](#)
- [Viewing the Product License, page 6-7](#)

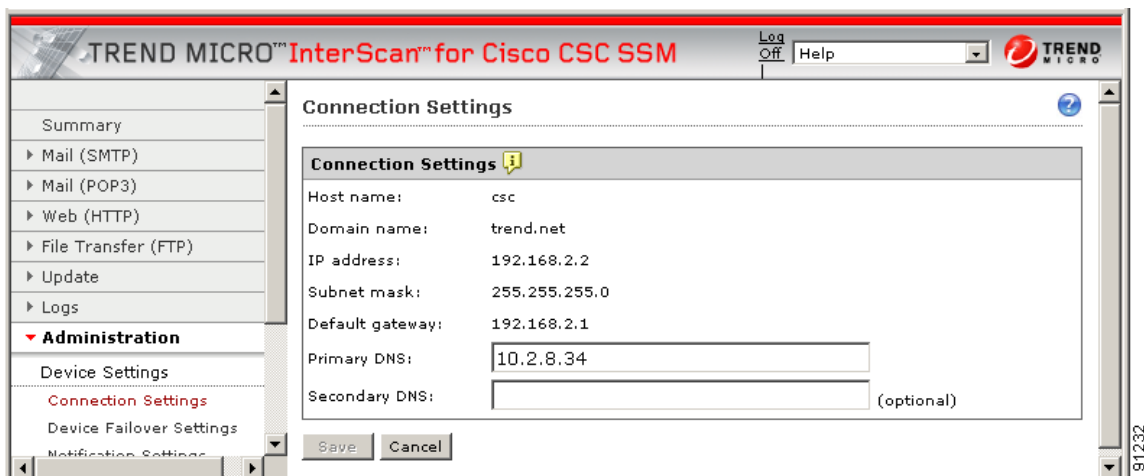
Configuring Connection Settings

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 choose **CSC Setup** from the menu.
- 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.

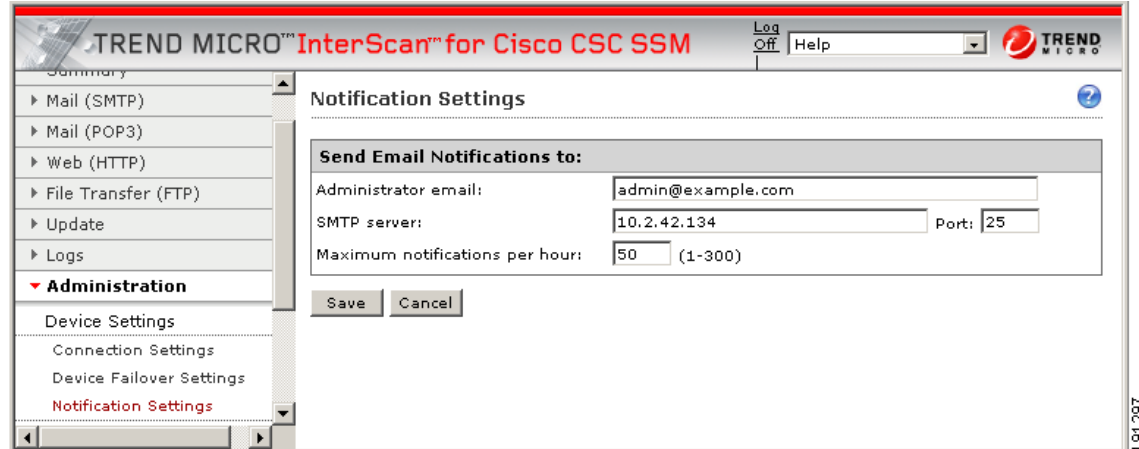
For more information, see the [“Reimaging the CSC SSM”](#) section on page A-5.

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 during installation on the Host Configuration window.
- 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 the ASDM. Choose **Configuration > Trend Micro Content Security**, and then choose **CSC Setup** from the menu.
-

**Note**

For more information about the Register to DCS and Register to TCM menu items, see [Using CSC SSM with Trend Micro Damage Cleanup Services, page C-1](#) and [Using CSC SSM with Trend Micro Control Manager, page B-1](#).

Backing Up Configuration Settings

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

- [Exporting a Configuration, page 6-4](#)
- [Importing a Configuration, page 6-4](#)

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 of the save.

**Note**

A configuration backup is essential for recovery in case you forget your ASDM or Web GUI password, depending on how you have set your password-reset policy. For more information, see [Recovering a Lost Password, page 8-5](#) and [Modifying the Password-reset Policy, page A-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 6-3](#).

Figure 6-3 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** You can open the file, called config.tgz, or save the file to your computer.
-

Importing a Configuration

To restore configuration settings, perform the following steps:

-
- Step 1** On 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 security 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: _____	<input type="checkbox"/> <input type="checkbox"/>
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 on, and choose Administration > Device Settings > Device Failover Settings .	<input type="checkbox"/>
Step 3	Open a second browser window and enter the following URL in the Address field: http://<secondary device IP address>:8443 . As in Step 2, log on, and choose Administration > Device Settings > Device Failover Settings .	<input type="checkbox"/>
Step 4	On 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: <code>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.</code> This message is normal behavior and appears because the peer is not yet configured.	<input type="checkbox"/>
Step 5	On 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: <code>InterScan for CSC SSM has successfully connected with the failover peer device.</code> Do not click anything else at this time for the secondary device.	<input type="checkbox"/>
Step 6	On 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: <code>Status: Last synchronized with peer on: 04/29/2007 15:20:11</code>	<input type="checkbox"/>

**Caution**

Be sure you do *not* click **Synchronize to peer** at the end of Step 5, while you are still on the Device Failover Settings window for the secondary device. If you do, the configuration you have already set up on the primary device is 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 [Installing Product Upgrades](#).

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.

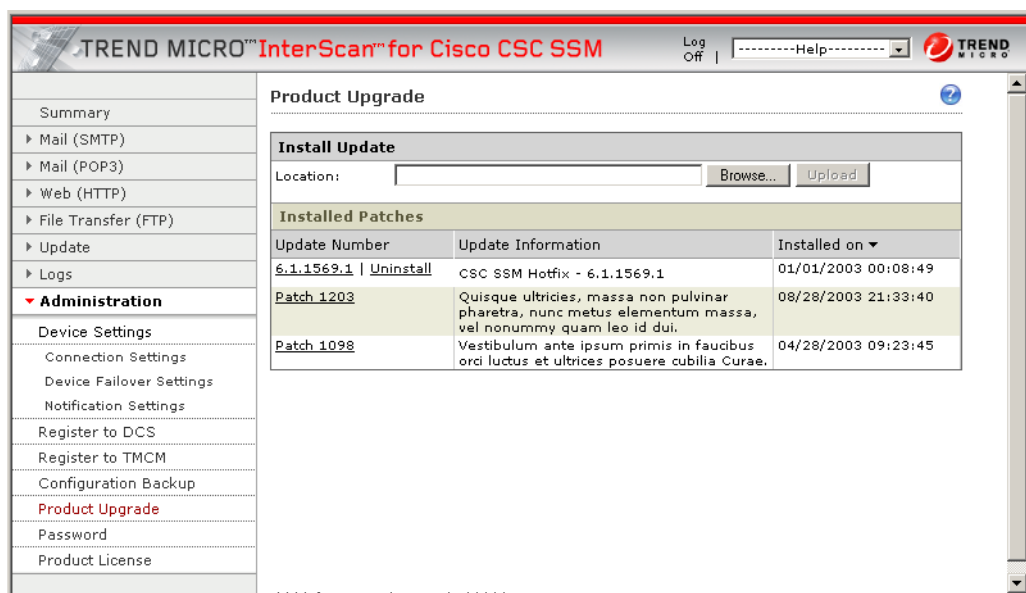
Installing Product Upgrades

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 6-4](#).

Figure 6-4 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

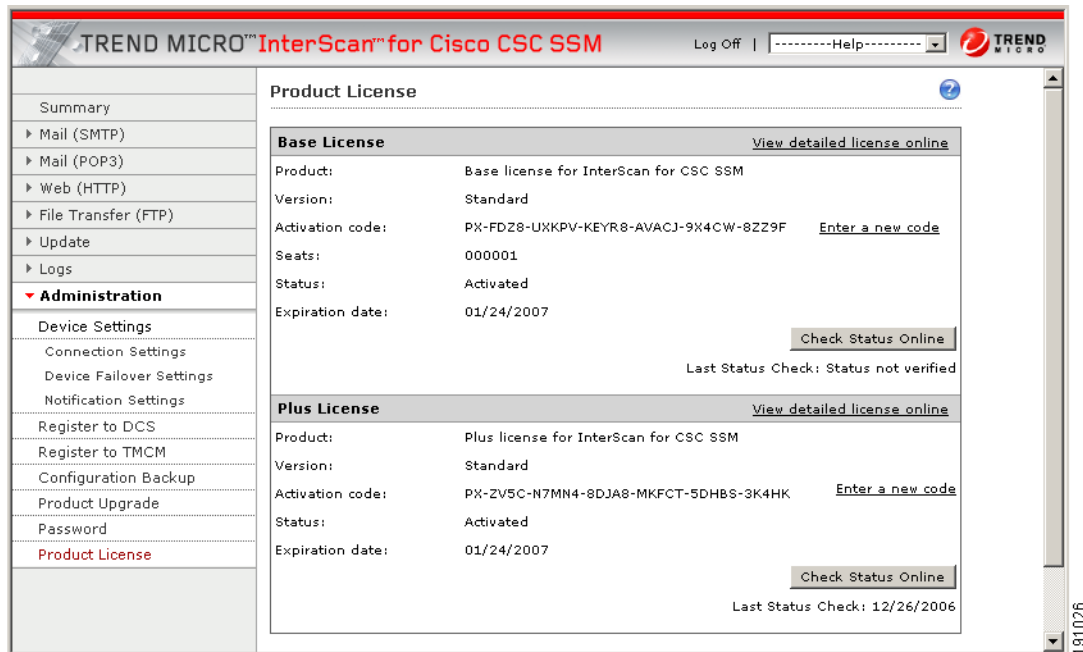
This section describes product licensing information, and includes the following topics:

- [License Expiration, page 6-8](#)
- [Licensing Information Links, page 6-9](#)
- [Renewing a License, page 6-9](#)

The Product License window (shown in [Figure 6-5](#)) allows you to view the status of your product license, which includes the following information:

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

Figure 6-5 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 short grace period. However, other features may become unavailable. For more information, see the [License Expiration](#) section.

License Expiration

As you approach and even pass the expiration date, a message appears in the Summary window under the window heading, similar to the example shown in [Figure 6-6](#).

Figure 6-6 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 Base 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:

-
- 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 in the previous figure.
-

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



Note For information about product activation, see the *ASDM User Guide*.

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 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.
-

