



# CHAPTER 31

## Configuring Trend Micro Content Security

---



### Note

The ASA 5580 does not support the CSC SSM feature.

---

This chapter describes how to configure the CSC SSM using the CSC Setup Wizard in ASDM and the CSC SSM GUI, and includes the following sections:

- [Information About the CSC SSM, page 31-1](#)
- [Licensing Requirements for the CSC SSM, page 31-2](#)
- [Prerequisites for the CSC SSM, page 31-2](#)
- [Guidelines and Limitations, page 31-3](#)
- [Default Settings, page 31-3](#)
- [CSC SSM Setup, page 31-3](#)
- [Using the CSC SSM GUI, page 31-13](#)
- [Where to Go Next, page 31-16](#)
- [Additional References, page 31-17](#)
- [Feature History for the CSC SSM, page 31-17](#)

## Information About the CSC SSM

The ASA 5500 series security appliance supports the CSC SSM, which runs Content Security and Control software. The CSC SSM provides protection against viruses, spyware, spam, and other unwanted traffic by scanning the FTP, HTTP, POP3, and SMTP packets that you configure the security appliance to send to it.

For more information about the CSC SSM, see the following URL:

<http://www.cisco.com/en/US/products/ps6823/index.html>

# Licensing Requirements for the CSC SSM

The following table shows the licensing requirements for this feature:

Model	License Requirement
ASA 5505	No support.
ASA 5510	Security Plus License: 2 contexts. <i>Optional license: 5 contexts.</i>
ASA 5520	Base License: 2 contexts. <i>Optional licenses: 5, 10, or 20 contexts.</i>
ASA 5540	Base License: 2 contexts. <i>Optional licenses: 5, 10, 20, or 50 contexts.</i>

For the ASA 5510, 5520, and 5540:

- With a Base License, the features enabled by default are SMTP virus scanning, POP3 virus scanning and content filtering, webmail virus scanning, HTTP file blocking, FTP virus scanning and file blocking, logging, and automatic updates.
- With a Security Plus License, the additional features enabled by default are SMTP anti-spam, SMTP content filtering, POP3 anti-spam, URL blocking, and URL filtering.

## Prerequisites for the CSC SSM

The CSC SSM has the following prerequisites:

- A CSC SSM card must be installed in the security appliance.
- A Product Authorization Key (PAK) for use in registering the CSC SSM.
- Activation keys that you receive by e-mail after you register the CSC SSM.
- The management port of the CSC SSM must be connected to your network to allow management and automatic updates of the CSC SSM software.
- The CSC SSM management port IP address must be accessible by the hosts used to run ASDM.
- You must obtain the following information to use in configuring the CSC SSM:
  - The CSC SSM management port IP address, netmask, and gateway IP address.
  - DNS server IP address.
  - HTTP proxy server IP address (needed only if your security policies require the use of a proxy server for HTTP access to the Internet).
  - Domain name and hostname for the CSC SSM.
  - An e-mail address and an SMTP server IP address and port number for e-mail notifications.
  - IP addresses of hosts or networks that are allowed to manage the CSC SSM. The IP addresses for the CSC SSM management port and the security appliance management interface can be in different subnets.
  - Password for the CSC SSM.

# Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

## Context Mode Guidelines

Supported in single and multiple context modes. In multiple-context mode, all panes under the CSC Setup node are available *only* in the admin context. You can restore the default password only in multiple-context mode in the system context.

## Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

## Failover Guidelines

Does not support sessions in Stateful Failover. The CSC SSM does not maintain connection information, and therefore cannot provide the failover unit with the required information. The connections that a CSC SSM is scanning are dropped when the security appliance in which the CSC SSM is installed fails. When the standby security appliance becomes active, it forwards the scanned traffic to the CSC SSM and the connections are reset.

## IPv6 Guidelines

Does not support IPv6.

## Model Guidelines

Supported on the ASA 5510, ASA 5520, and ASA 5540 only.

# Default Settings

[Table 31-1](#) lists the default settings for the CSC SSM.

**Table 31-1** *Default CSC SSM Parameters*

Parameter	Default
FTP inspection on the security appliance	Enabled
All features included in the license(s) that you have purchased	Enabled

# CSC SSM Setup

The CSC Setup Wizard lets you configure basic operational parameters for the CSC SSM. You must complete this wizard at least once before you can configure options in each screen separately. After you complete the CSC Setup Wizard, you can modify each screen individually without using this wizard again.

Additionally, you cannot access the panes under Configuration > Trend Micro Content Security > CSC Setup or under Monitoring > Trend Micro Content Security > Content Security until you complete the CSC Setup Wizard. If you try to access these panes before completing this wizard, a dialog box appears and lets you access the wizard directly to complete the configuration.

This section includes the following topics:

- [Activation/License, page 31-4](#)
- [IP Configuration, page 31-5](#)
- [Host/Notification Settings, page 31-5](#)
- [Management Access Host/Networks, page 31-6](#)
- [Password, page 31-7](#)
- [Restoring the Default Password, page 31-7](#)
- [Wizard Setup, page 31-8](#)

## Activation/License

The Activation/License pane lets you review or renew activation codes for the CSC SSM Base License and the Plus License.

You can use ASDM to configure CSC licenses only once each for the two licenses. Renewed license activation codes are downloaded automatically with scheduled software updates. Links to the licensing status pane and the CSC UI home pane appear at the bottom of this window. The serial number for the assigned license is filled in automatically.

To review license status or renew a license, perform the following steps:

- 
- Step 1** The Activation/License pane shows the following display-only information for the Base License and the Plus License:
- The name of the component.
  - The activation code for the corresponding Product field.
  - The status of the license. If the license is valid, the expiration date appears. If the expiration date has passed, this field indicates that the license has expired.
  - The maximum number of network devices that the Base License supports. The Plus License does not affect the number of network devices supported; therefore, the Nodes field does not appear in the Plus License area.
- Step 2** To review license status or renew your license, click the link provided.
- Step 3** To go to the CSC home pane in ASDM, click the link provided.
- 

### What to Do Next

See the [“IP Configuration”](#) section on page 31-5.

## IP Configuration

The IP Configuration pane lets you configure management access for the CSC SSM, the DNS servers it should use, and a proxy server for retrieving CSC SSM software updates.

To configure management access and other related details for the CSC SSM, perform the following steps:

- 
- Step 1** Set the following parameters for management access to the CSC SSM:
- Enter the IP address for management access to the CSC SSM.
  - Enters the netmask for the network containing the management IP address of the CSC SSM.
  - Enter the IP address of the gateway device for the network that includes the management IP address of the CSC SSM.
- Step 2** Set parameters of the DNS servers for the network that includes the management IP address of the CSC SSM.
- Enter the IP address of the primary DNS server.
  - (Optional) Enter the IP address of the secondary DNS server.
- Step 3** (Optional) Enter parameters for an HTTP proxy server, used by the CSC SSM to contact a CSC SSM software update server. If your network configuration does not require the CSC SSM to use a proxy server, leave the fields in this group blank.
- Enter the IP address of the proxy server.
  - Enter the listening port of the proxy server.
- 

### What to Do Next

See the [“Host/Notification Settings”](#) section on page 31-5.

## Host/Notification Settings

The Host/Notification Settings pane lets you configure details about hostname, domain name, e-mail notifications, and a domain name for e-mail to be excluded from detailed scanning.

To configure host and notification settings, perform the following steps:

- 
- Step 1** In the Host and Domain Names area, set the hostname and domain name of the CSC SSM.
- Step 2** In the Incoming E-mail Domain Name area, set the trusted incoming e-mail domain name for SMTP-based e-mail. The CSC SSM scans SMTP e-mail sent to this domain. The types of threats that the CSC SSM scans for depend on the license that you purchased for the CSC SSM and the configuration of the CSC SSM software.



**Note** CSC SSM lets you configure a list of many incoming e-mail domains. ASDM displays only the first domain in the list. To configure additional incoming e-mail domains, access the CSC SSM interface. To do so, choose **Configuration > Trend Micro Content Security > CSC Setup > Mail**, and then click one of the links. After logging in to the CSC SSM, choose **Mail (SMTP) > Configuration**, and then click the **Incoming Mail** tab.

**Step 3** Configure the following settings for e-mail notification of events:

- The administrator e-mail address for the account to which notification e-mails should be sent.
- The IP address of the SMTP server.
- The port to which the SMTP server listens.

### What to Do Next

See the [“Management Access Host/Networks”](#) section on page 31-6.

## Management Access Host/Networks

The Management Access Host/Networks pane lets you specify the hosts and networks for which management access to the CSC SSM is permitted. You must specify at least one permitted host or network, up to a maximum of eight permitted hosts or networks.

To specify hosts and networks for which management access to the CSC SSM is allowed, perform the following steps:

**Step 1** Enter the IP address of a host or network that you want to add to the Selected Hosts/Network list.

**Step 2** Enter the netmask for the host or network that you specified in the IP Address field.



**Note** To allow all hosts and networks, enter **0.0.0.0** in the IP Address field, and choose 0.0.0.0 from the Mask list.

The Selected Hosts/Networks list displays the hosts or networks trusted for management access to the CSC SSM.

**Step 3** To add the host or network that you specified in the IP Address field in the Selected Hosts/Networks list, click **Add**.

**Step 4** To remove a host or network from the Selected Hosts/Networks list, choose an entry from the list and click **Delete**.

### What to Do Next

See the [“Password”](#) section on page 31-7.

## Password

The Password pane lets you change the password required for management access to the CSC SSM. The CSC SSM has a password that is maintained separately from the ASDM password. You can configure them to be identical; however, changing the CSC SSM password does not affect the ASDM password.

If ASDM is connected to the CSC SSM and you change the CSC SSM password, the connection to the CSC SSM is dropped. As a result, ASDM displays a confirmation dialog box that you must respond to before the password is changed.

**Tip**

Whenever the connection to the CSC SSM is dropped, you can reestablish it. To do so, click the **Connection to Device** icon on the status bar to display the Connection to Device dialog box, and then click **Reconnect**. ASDM prompts you for the CSC SSM password, which is the new password that you have defined.

Passwords must be 5 - 32 characters long.

Passwords appears as asterisks when you type them.

**Note**

The default password is "cisco."

To change the password required for management access to the CSC SSM, perform the following steps:

- Step 1** In the Old Password field, enter the current password for management access to the CSC SSM.
- Step 2** In the New Password field, enter the new password for management access to the CSC SSM.
- Step 3** In the Confirm New Password field, reenter the new password for management access to the CSC SSM.

### What to Do Next

If required, see the ["Restoring the Default Password" section on page 31-7](#).

See the ["Wizard Setup" section on page 31-8](#).

## Restoring the Default Password

You can use ASDM to reset the CSC SSM password. You can reset this password to the default value, which is "cisco" (excluding quotation marks). If the CSC password-reset policy has been set to "Denied," then you cannot reset the password through the ASDM CLI. To change this policy, you must access the CSC SSM through the security appliance CLI by entering the **session** command. For more information, see the *Trend Micro InterScan for Cisco CSC SSM Administrator Guide*.

**Note**

This option does not appear in the menu if an SSM is not installed.

To reset the CSC SSM password to the default value, perform the following steps:

- Step 1** From the ASDM menu bar, choose **Tools > CSC Password Reset**.

The CSC Password Reset confirmation dialog box appears.

**Step 2** Click **OK** to reset the CSC SSM password to the default value.

A dialog box appears, indicating the success or failure of the password reset. If the password was not reset, make sure you are using Version 8.0(2) software on the security appliance and the most recent Version 6.1.x software on the CSC SSM.

**Step 3** Click **Close** to close the dialog box.

**Step 4** After you have reset the password, you should change it to a unique value.

---

## What to Do Next

See the “[Password](#)” section on page 31-7.

## Wizard Setup

The Wizard Setup screen lets you start the CSC Setup Wizard. To start the CSC Setup Wizard, click **Launch Setup Wizard**.

Before you can directly access any of the other screens under CSC Setup, you must complete the CSC Setup Wizard. This wizard includes the following screens:

- [CSC Setup Wizard Activation Codes Configuration, page 31-8](#)
- [CSC Setup Wizard IP Configuration, page 31-9](#)
- [CSC Setup Wizard Host Configuration, page 31-9](#)
- [CSC Setup Wizard Management Access Configuration, page 31-10](#)
- [CSC Setup Wizard Password Configuration, page 31-10](#)
- [CSC Setup Wizard Traffic Selection for CSC Scan, page 31-10](#)
- [CSC Setup Wizard Summary, page 31-12](#)

After you complete the CSC Setup Wizard once, you can change any settings in screens related to the CSC SSM without using the CSC Setup Wizard again.

## CSC Setup Wizard Activation Codes Configuration

To display the activation codes that you have entered to enable features on the CSC SSM, perform the following steps:

Choose **Configuration > Trend Micro Content Security > CSC Setup > Activation/License**.

The activation code settings that you have made appear on this screen, according to the type of license you have, as follows:

- The activation code for the Base License appears. The Base License includes anti-virus, anti-spyware, and file blocking.
- The activation code for the Plus License appears, if you have entered one. If not, this field is blank. The Plus License includes anti-spam, anti-phishing, content filtering, URL blocking and filtering, and web reputation.

## What to Do Next

See the [“CSC Setup Wizard IP Configuration”](#) section on page 31-9.

## CSC Setup Wizard IP Configuration

To display the IP configuration settings that you have entered for the CSC SSM, perform the following steps:

Choose **Configuration > Trend Micro Content Security > CSC Setup > IP Configuration**.

The IP configuration settings that you have entered for the CSC SSM appear, including the following:

- The IP address for the management interface of the CSC SSM.
- The network mask for the management interface of the CSC SSM that you have selected from the drop-down list.
- The IP address of the gateway device for the network that contains the CSC SSM management interface.
- The primary DNS server IP address.
- The secondary DNS server IP address (if configured).
- The proxy server (if configured).
- The proxy port (if configured).

## What to Do Next

See the [“CSC Setup Wizard IP Configuration”](#) section on page 31-9.

## CSC Setup Wizard Host Configuration

To display the host configuration settings that you have entered for the CSC SSM, perform the following steps:

Choose **Configuration > Trend Micro Content Security > CSC Setup > Host Configuration**.

The host configuration settings that you have entered for the CSC SSM appear, including the following:

- The hostname of the CSC SSM.
- The name of the domain in which the CSC SSM resides.
- The domain name for incoming e-mail.
- The e-mail address of the domain administrator.
- The IP address of the e-mail server.
- The port number through which you connect to the CSC SSM.

## What to Do Next

See the [“CSC Setup Wizard Management Access Configuration”](#) section on page 31-10.

## CSC Setup Wizard Management Access Configuration

To display the subnet and host settings that you have entered to grant access to the CSC SSM, perform the following steps:

---

**Step 1** Choose **Configuration > Trend Micro Content Security > CSC Setup > Management Access Configuration**.

The management access configuration settings that you have entered for the CSC SSM appear, including the following:

- The IP address for networks and hosts that are allowed to connect to the CSC SSM.
- The network mask for networks and hosts that are allowed to connect to the CSC SSM that you have selected from the drop-down list.

**Step 2** To add the IP address of the networks and hosts that you want to allow to connect to the CSC SSM, click **Add**.

**Step 3** To remove the IP address of a network or host whose ability to connect to the CSC SSM you no longer want, click **Delete**.

The Selected Hosts/Networks table lists the IP addresses of networks and hosts whose connection to the CSC SSM you have added.

---

### What to Do Next

See the [“CSC Setup Wizard Password Configuration”](#) section on page 31-10.

## CSC Setup Wizard Password Configuration

To change the password required for management access to the CSC SSM, perform the following steps:

---

**Step 1** Choose **Configuration > Trend Micro Content Security > CSC Setup > Password**.

**Step 2** In the Old Password field, enter the current password for management access to the CSC SSM.

**Step 3** In the New Password field, enter the new password for management access to the CSC SSM.

**Step 4** In the Confirm New Password field, reenter the new password for management access to the CSC SSM.

---

### What to Do Next

See the [“CSC Setup Wizard Traffic Selection for CSC Scan”](#) section on page 31-10.

## CSC Setup Wizard Traffic Selection for CSC Scan

To display the settings that you have made to select traffic for CSC scanning, perform the following steps:

---

**Step 1** Choose **Configuration > Trend Micro Content Security > CSC Setup > Traffic Selection for CSC Scan**.

The traffic selection for CSC scanning configuration settings that you have entered for the CSC SSM appear, including the following:

- The interface to the CSC SSM that you have chosen from the drop-down list.
- The source of network traffic for the CSC SSM to scan.
- The destination of network traffic for the CSC SSM to scan.
- The source or destination service for the CSC SSM to scan.

**Step 2** Do one of the following:

- To specify additional traffic details for CSC scanning, click **Add**. For more information, see [“Specifying Traffic for CSC Scanning” section on page 31-11](#).
  - To modify additional traffic details for CSC scanning, click **Edit**. For more information, see [“Specifying Traffic for CSC Scanning” section on page 31-11](#).
  - To remove additional traffic details for CSC scanning, click **Delete**.
- 

## Specifying Traffic for CSC Scanning

To define, modify, or remove additional settings for selecting traffic for CSC scanning, perform the following steps:

- 
- Step 1** In the Traffic Selection for CSC Scan screen, click **Specify traffic for CSC Scan**.  
The Specify traffic for CSC Scan dialog box appears.
- Step 2** Choose the type of interface to the CSC SSM from the drop-down list. Available settings are global (all interfaces), inside, management, and outside.
- Step 3** Choose the source of network traffic for the CSC SSM to scan from the drop-down list.
- Step 4** Choose the destination of network traffic for the CSC SSM to scan from the drop-down list.
- Step 5** Choose the type of service for the CSC SSM to scan from the drop-down list.
- Step 6** Enter a description for the network traffic that you define for the CSC SSM to scan.
- Step 7** Specify whether or not to allow the CSC SSM to scan network traffic if the CSC card fails. Choose one of the following options:
- To allow traffic through without being scanned, click **Permit**.
  - To prevent traffic from going through without being scanned, click **Close**.
- Step 8** Click **OK** to save your settings.  
The added traffic details appear on the CSC Setup Wizard Traffic selection for CSC Scan screen.
- Step 9** Click **Cancel** to discard these settings and return to the CSC Setup Wizard Traffic selection for CSC Scan screen. If you click **Cancel**, ASDM displays a dialog box to confirm your decision.
- 

## What to Do Next

See the [“CSC Setup Wizard Summary” section on page 31-12](#).

## CSC Setup Wizard Summary

To review the settings that you have made with the CSC Setup Wizard, perform the following steps:

---

**Step 1** Choose **Configuration > Trend Micro Content Security > CSC Setup > Summary**.

The CSC Setup Wizard Summary screen shows the following display-only settings:

- The settings that you made in the Activation Codes Configuration screen, including the Base License activation code and the Plus License activation code, if you entered one. If not, this field is blank.
- The settings that you made in the IP Configuration screen, including the following information:
  - IP address and netmask for the management interface of the CSC SSM.
  - IP address of the gateway device for the network that includes the CSC SSM management interface.
  - Primary DNS server IP address.
  - Secondary DNS server IP address (if configured).
  - Proxy server and port (if configured).
- The settings that you made in the Host Configuration screen, including the following information:
  - Hostname of the CSC SSM.
  - Domain name for the domain that includes the CSC SSM.
  - Domain name for incoming e-mail.
  - Administrator e-mail address.
  - E-mail server IP address and port number.
- The settings that you made on the Management Access Configuration screen. The drop-down list includes the hosts and networks from which the CSC SSM allows management connections.
- Indicates whether or not you have changed the password in the Password Configuration screen.

**Step 2** (Optional) Click **Back** to return to the previous screens of the CSC Setup Wizard to change any settings.



---

**Note** The Next button is dimmed; however, if you click **Back** to access any of the preceding screens in this wizard, click **Next** to return to the Summary screen.

---

**Step 3** Click **Finish** to complete the CSC Setup Wizard and save all settings that you have specified. After you click **Finish**, you can change any settings related to the CSC SSM without using the CSC Setup Wizard again.

A summary of the status of commands that were sent to the device appears.

**Step 4** Click **Close** to close this screen, and then click **Next**.

A message appears indicating that the CSC SSM has been activated and is ready for use.

**Step 5** (Optional) Click **Cancel** to exit the CSC Setup Wizard without saving any of the selected settings. If you click **Cancel**, a dialog box appears to confirm your decision.

---

## What to Do Next

See the “Using the CSC SSM GUI” section on page 31-13.

# Using the CSC SSM GUI

This section describes how to configure features using the CSC SSM GUI, and includes the following topics:

- [Web, page 31-13](#)
- [Mail, page 31-14](#)
- [File Transfer, page 31-15](#)
- [Updates, page 31-16](#)

## Web



### Note

---

To access the CSC SSM, you must reenter the CSC SSM password. Sessions in the CSC SSM browser time out after ten minutes of inactivity. If you close the CSC SSM browser and click another link in ASDM, you are not prompted for the CSC SSM password again, because one session is already open.

---

To view whether or not web-related features are enabled and access the CSC SSM GUI for configuring these features, perform the following steps:

- 
- Step 1** Choose **Configuration > Trend Micro Content Security > Web**.
- The URL Blocking and Filtering area is display-only and shows whether or not URL blocking is enabled on the CSC SSM.
- Step 2** Click **Configure URL Blocking** to open a screen for configuring URL blocking on the CSC SSM.
- The URL Filtering area is display-only and shows whether or not URL filtering is enabled on the CSC SSM.
- Step 3** Click **Configure URL Filtering** to open a screen for configuring URL filtering rules on the CSC SSM.
- The File Blocking area is display-only and shows whether or not URL file blocking is enabled on the CSC SSM.
- Step 4** Click **Configure File Blocking** to open a screen for configuring file blocking settings on the CSC SSM.
- The HTTP Scanning area is display-only and shows whether or not HTTP scanning is enabled on the CSC SSM.
- Step 5** Click **Configure Web Scanning** to open a screen for configuring HTTP scanning settings on the CSC SSM.
- The Web Reputation area is display-only and shows whether or not the Web Reputation service is enabled on the CSC SSM.
- Step 6** Click **Configure Web Reputation** to open a screen for configuring the Web Reputation service on the CSC SSM.
-

## What to Do Next

See the “Mail” section on page 31-14.

# Mail

The Mail pane lets you see whether or not e-mail-related features are enabled and lets you access the CSC SSM GUI to configure these features. To configure e-mail related features, choose **Configuration > Trend Micro Content Security > Mail**.

This section includes the following topics:

- [SMTP Tab, page 31-14](#)
- [POP3 Tab, page 31-15](#)

## SMTP Tab

**Note**

To access the CSC SSM, you must reenter the CSC SSM password. Sessions in the CSC SSM browser time out after ten minutes of inactivity. If you close the CSC SSM browser and click another link in ASDM, you are not prompted for the CSC SSM password again, because one session is already open.

To configure SMTP scanning, perform the following steps:

- 
- Step 1** Click the **SMTP Tab**.
  - Step 2** The Incoming Scan area is display-only and shows whether or not the incoming SMTP scanning feature is enabled on the CSC SSM. Click **Configure Incoming Scan** to open a screen for configuring incoming SMTP scan settings on the CSC SSM.
  - Step 3** The Outgoing Scan area is display-only and shows whether or not the outgoing SMTP scanning feature is enabled on the CSC SSM. Click **Configure Outgoing Scan** to open a screen for configuring outgoing SMTP scan settings on the CSC SSM.
  - Step 4** The Incoming Filtering area is display-only and shows whether or not content filtering for incoming SMTP e-mail is enabled on the CSC SSM. Click **Configure Incoming Filtering** to open a screen for configuring incoming SMTP e-mail content filtering settings on the CSC SSM.
  - Step 5** The Outgoing Filtering area is display-only and shows whether or not content filtering for outgoing SMTP e-mail is enabled on the CSC SSM. Click **Configure Outgoing Filtering** to open a screen for configuring outgoing SMTP e-mail content filtering settings on the CSC SSM.
  - Step 6** The Anti-spam area is display-only and shows whether or not the SMTP anti-spam feature is enabled on the CSC SSM. Click **Configure Anti-spam** to open a screen for configuring SMTP anti-spam settings, including E-mail Reputation, on the CSC SSM.
-

## POP3 Tab

**Note**

To access the CSC SSM, you must reenter the CSC SSM password. Sessions in the CSC SSM browser time out after ten minutes of inactivity. If you close the CSC SSM browser and click another link in ASDM, you are not prompted for the CSC SSM password again, because one session is already open.

To configure POP3 scanning, perform the following steps:

- 
- Step 1** Click the **POP3** Tab.
  - Step 2** The Scanning area is display-only and shows whether or not POP3 e-mail scanning is enabled on the CSC SSM. Click **Configure Scanning** to open a window for configuring POP3 e-mail scanning on the CSC SSM.
  - Step 3** The Anti-spam area is display-only and shows whether or not the POP3 anti-spam feature is enabled on the CSC SSM. Click **Configure Anti-spam** to open a window for configuring the POP3 anti-spam feature on the CSC SSM.
  - Step 4** The Content Filtering area is display-only and shows whether or not POP3 e-mail content filtering is enabled on the CSC SSM. Click **Configure Content Filtering** to open a window for configuring POP3 e-mail content filtering on the CSC SSM.
- 

### What to Do Next

See the [“File Transfer” section on page 31-15](#).

## File Transfer

The File Transfer pane lets you view whether or not FTP-related features are enabled and lets you access the CSC SSM for configuring FTP-related features.

**Note**

To access the CSC SSM, you must reenter the CSC SSM password. Sessions in the CSC SSM browser time out after ten minutes of inactivity. If you close the CSC SSM browser and click another link in ASDM, you are not prompted for the CSC SSM password again, because one session is already open.

To view the status or configure FTP-related features, perform the following steps:

- 
- Step 1** Click the **File Transfer** tab.  
The File Scanning area is display-only and shows whether or not FTP file scanning is enabled on the CSC SSM.
  - Step 2** Click **Configure File Scanning** to open a window for configuring FTP file scanning settings on the CSC SSM.  
The File Blocking area is display-only and shows whether or not FTP blocking is enabled on the CSC SSM.

- Step 3** Click **Configure File Blocking** to open a window for configuring FTP file blocking settings on the CSC SSM.
- 

### What to Do Next

See the [“Updates” section on page 31-16](#).

## Updates

The Updates pane lets you view whether or not scheduled updates are enabled and lets you access the CSC SSM for configuring scheduled updates.



### Note

To access the CSC SSM, you must reenter the CSC SSM password. Sessions in the CSC SSM browser time out after ten minutes of inactivity. If you close the CSC SSM browser and click another link in ASDM, you are not prompted for the CSC SSM password again, because one session is already open.

---

To view the status or configure scheduled update settings, perform the following steps:

---

- Step 1** Click the **Updates** tab.

The Scheduled Updates area is display-only and shows whether or not scheduled updates are enabled on the CSC SSM.

The Scheduled Update Frequency area displays information about when updates are scheduled to occur, such as “Hourly at 10 minutes past the hour.”

The Component area displays names of parts of the CSC SSM software that can be updated.

In the Components area, the Scheduled Updates area is display-only and shows whether or not scheduled updates are enabled for the corresponding components.

- Step 2** Click **Configure Updates** to open a window for configuring scheduled update settings on the CSC SSM.
- 



### Note

If you restart the security appliance, the SSM is not automatically restarted. For more information, see the [“Managing SSMs and SSCs” section in the \*Cisco ASA 5500 Series Configuration Guide using the CLI\*](#).

---

## Where to Go Next

See the [“Monitoring Trend Micro Content Security” section on page 49-1](#).

## Additional References

For additional information related to implementing the CSC SSM, see the following documents:

Related Topic	Document Title
Instructions on use of the CSC SSM GUI. Additional licensing requirements of specific windows available in the CSC SSM GUI. Reviewing the default content security policies in the CSC SSM GUI before modifying them or entering advanced configuration settings.	<i>Trend Micro InterScan for Cisco CSC SSM Administrator Guide</i>
Accessing ASDM for the first time and assistance with the Startup Wizard.	<i>Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide</i>
Assistance with SSM hardware installation and connection to the security appliance.	<i>Cisco ASA 5500 Series Hardware Installation Guide</i>
Technical Documentation, Marketing, and Support-related information	See <a href="http://www.cisco.com/en/US/products/ps6823/index.html">http://www.cisco.com/en/US/products/ps6823/index.html</a> .

## Feature History for the CSC SSM

Table 31-2 lists the release history for this feature.

**Table 31-2** Feature History for the CSC SSM

Feature Name	Releases	Feature Information
CSC SSM	ASA 7.0(1), ASDM 5.0(1)	The CSC SSM runs Content Security and Control software, which provides protection against viruses, spyware, spam, and other unwanted traffic.  The following commands were introduced: <b>csc {fail-close   fail-open}</b> , <b>hw-module module 1 [recover   reload   reset   shutdown]</b> , <b>session</b> , <b>show module [all   slot [details   recover]]</b> .
Password reset	ASA 7.2(2), ASDM 5.2(2)	The <b>hw-module module password-reset</b> command was introduced.
CSC SSM	ASA 8.1(1), ASDM 6.1(1) and ASA 8.1(2), ASDM 6.1(2)	This feature is not supported.
Syslog format	ASA 8.3(1), ASDM 6.3(1)	CSC syslog format is consistent with the security appliance syslog format. Syslog message explanations have been added to the <i>Trend Micro InterScan for Cisco CSC SSM Administrator Guide</i> . The source and destination IP information has been added to the ASDM Log Viewer GUI. All syslog messages include predefined syslog priorities and cannot be configured through the CSC SSM GUI.

