

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, and includes the following sections:

- [Connecting to the CSC SSM, page 29-1](#)
- [Managing the CSC SSM, page 29-2](#)
- [CSC SSM Setup, page 29-9](#)
- [Web, page 29-21](#)
- [Mail, page 29-22](#)
- [File Transfer, page 29-24](#)
- [Updates, page 29-25](#)

Connecting to the CSC SSM

With each session you start in ASDM, the first time you access features related to the CSC SSM, you must specify the management IP address and provide the password for the CSC SSM. After you successfully connect to the CSC SSM, you are not prompted again for the management IP address and password. If you start a new ASDM session, the connection to the CSC SSM is reset and you must specify the IP address and the CSC SSM password again. The connection to the CSC SSM is also reset if you change the time zone on the adaptive security appliance.

**Note**

The CSC SSM has a password that is maintained separately from the ASDM password. You can configure the two passwords to be identical, but changing the CSC SSM password does not affect the ASDM password.

To connect to the CSC SSM, perform the following steps:

-
- Step 1** In the main ASDM application window, click the **Content Security** tab.
- Step 2** In the Connecting to CSC dialog box, choose one of the following options:
- **Management IP Address**—Connects to the IP address of the management port on the SSM. ASDM automatically detects the IP address for the SSM in the adaptive security appliance. If this detection fails, you can specify the management IP address manually.

- Other IP Address or Hostname—Connects to an alternate IP address or hostname on the SSM.

Step 3 Enter the port number in the Port field, and then click **Continue**.

Step 4 In the CSC Password dialog box, type your CSC password, and then click **OK**.



Note If you have not completed the CSC Setup Wizard (choose **Configuration > Trend Micro Content Security > CSC Setup > Wizard Setup**), complete the configuration in the CSC Setup Wizard, which includes changing the default password, “cisco.”

For ten minutes after you have entered the password, you do not need to reenter the CSC SSM password to access other parts of the CSC SSM GUI.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

Managing the CSC SSM

This section describes how to manage the CSC SSM, and includes the following topics:

- [About the CSC SSM, page 29-2](#)
- [Getting Started with the CSC SSM, page 29-4](#)
- [Determining What Traffic to Scan, page 29-6](#)
- [Rule Actions for CSC Scanning, page 29-8](#)

About the CSC SSM

ASDM lets you configure activation codes and other, basic operational parameters for the Content Security and Control (CSC) SSM, as well as CSC-related features. The ASA 5500 series adaptive 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. It accomplishes this by scanning the FTP, HTTP, POP3, and SMTP traffic that you configure on the adaptive security appliance to send to it.

[Figure 29-1](#) illustrates the flow of traffic through an adaptive security appliance that has the following:

- A CSC SSM installed and configured.

- A service policy that determines which traffic is diverted to the SSM for scans.

In this example, the client could be a network user who is accessing a website, downloading files from an FTP server, or retrieving e-mail from a POP3 server. SMTP scans differ in that you should configure the adaptive security appliance to scan traffic sent from outside to SMTP servers protected by the adaptive security appliance.

**Note**

The CSC SSM can scan FTP file transfers only when FTP inspection is enabled on the adaptive security appliance. By default, FTP inspection is enabled.

Figure 29-1 *Flow of Scanned Traffic with CSC SSM*



You use ASDM for system setup and monitoring of the CSC SSM. To configure content security policies in the CSC SSM software, you click links within ASDM to access the web-based GUI for the CSC SSM. The CSC SSM GUI appears in a separate web browser window. To access the CSC SSM, you must enter the CSC SSM password. To use the CSC SSM GUI, see the *Trend Micro InterScan for Cisco CSC SSM Administrator Guide*.

**Note**

ASDM and the CSC SSM maintain separate passwords. You can configure their passwords to be identical; however, changing one of these two passwords does not affect the other password.

The connection between the host running ASDM and the adaptive security appliance is made through a management port on the adaptive security appliance. The connection to the CSC SSM GUI is made through the SSM management port. Because these two connections are required to manage the CSC SSM, any host running ASDM must be able to reach the IP address of both the adaptive security appliance management port and the SSM management port.

[Figure 29-2](#) shows an adaptive security appliance with a CSC SSM that is connected to a dedicated management network. Although a dedicated management network is not required, we recommend that you use one. This figure includes the following:

- An HTTP proxy server is connected to the inside network and to the management network to enable the CSC SSM to contact the Trend Micro Update Server.

- The management port of the adaptive security appliance is connected to the management network. To allow management of the adaptive security appliance and the CSC SSM, hosts running ASDM must be connected to the management network.
- The management network includes an SMTP server for e-mail notifications for the CSC SSM and a syslog server to which the CSC SSM can send system log messages.

Figure 29-2 *CSC SSM Deployment with a Management Network*



Getting Started with the CSC SSM

Before you receive the security benefits that by a CSC SSM provides, you must perform several steps in addition to SSM hardware installation.

To configure the adaptive security appliance and the CSC SSM, perform the following steps:

-
- Step 1** If the CSC SSM was not pre-installed in a Cisco ASA 5500 series adaptive security appliance, install the CSC SSM and connect a network cable to the SSM management port. For assistance with SSM installation and connection, see the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

The CSC SSM management port must be connected to your network to allow management of and automatic updates to the CSC SSM software. Additionally, the CSC SSM uses the management port for e-mail notifications and syslog message generation.

- Step 2** With the CSC SSM, you received a Product Authorization Key (PAK). Use the PAK to register the CSC SSM at the following URL:

<http://www.cisco.com/go/license>

After you register, you will receive activation keys by e-mail. The activation keys are required before you can complete [Step 5](#).

- Step 3** Obtain the following information, for use in [Step 5](#).

- Activation keys, received after completing [Step 2](#).
- The SSM management port IP address, netmask, and gateway IP address. The SSM management port IP address must be accessible by the hosts used to run ASDM. The IP addresses for the SSM management port and the adaptive security appliance management interface can be in different subnets.
- DNS server IP address.
- HTTP proxy server IP address (necessary only if your security policies require use of a proxy server for HTTP access to the Internet).
- Domain name and hostname for the 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.
- Password for the CSC SSM.

Step 4 In ASDM, verify time settings on the security appliance. Time setting accuracy is important for logging of security events and for automatic updates of the CSC SSM software.

- If you manually control time settings, verify the clock settings, including time zone. Choose **Configuration > Device Setup > System Time > Clock**.
- If you are using NTP, verify the NTP configuration. Choose **Configuration > Device Setup > System Time > NTP**.

Step 5 Complete the CSC Setup Wizard.

- Choose **Configuration > Trend Micro Content Security**. Connect to and log in to the CSC SSM. Choose **CSC Setup > Wizard Setup**, and then click **Launch Setup Wizard**.
- If you are rerunning the CSC Setup Wizard, perform the same steps listed in the previous bullet:

For assistance with the CSC Setup Wizard, click **Help**.

Step 6 Configure service policies to divert to the CSC SSM the traffic that you want scanned.

If you create a global policy to divert traffic for scans, all traffic (inbound and outbound) for the supported protocols is scanned. To maximize performance of the adaptive security appliance and the CSC SSM, scan traffic only from untrusted sources.

To view best practices for diverting traffic to the CSC SSM, see [Determining What Traffic to Scan, page 29-6](#).

If you want to create a global policy that diverts traffic for scans, perform the following steps:

- a. Choose **Configuration > Firewall > Service Policy Rules**, and then click **Add**.
The Add Service Policy Rule Wizard screen appears.
- b. Click the **Global - applies to all interfaces** option, and then click **Next**.
The Traffic Classification Criteria screen appears.
- c. Click the **Create a new traffic class** option, type a name for the traffic class in the adjacent field, check the **Any traffic** check box, and then click **Next**.
The Rule Actions screen appears.
- d. Click the **CSC Scan** tab, and then check the **Enable CSC scan for this traffic flow** check box.
- e. Choose whether the adaptive security appliance should permit or deny selected traffic to pass if the CSC SSM is unavailable by making the applicable selection in the area labeled: **If CSC card fails, then**.
- f. Click **Finish**.

The new service policy appears in the Service Policy Rules pane.

g. Click **Apply.**

The adaptive security appliance begins diverting traffic to the CSC SSM, which performs the content security scans that have been enabled according to the license that you purchased.

Step 7 (Optional) Review the default content security policies in the CSC SSM GUI. The default content security policies are suitable for most implementations. Modifying them requires advanced configuration that you should perform only after reading the *Trend Micro InterScan for Cisco CSC SSM Administrator Guide*.



Note

You review the content security policies by viewing the enabled features in the CSC SSM GUI. The availability of features depends on the license that you purchased. By default, all features included in the license that you purchased are enabled.

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 Plus License, the additional features enabled by default are SMTP anti-spam, SMTP content filtering, POP3 anti-spam, URL blocking, and URL filtering.

To access the CSC SSM GUI in ASDM, choose **Configuration > Trend Micro Content Security**, and then click one of the following links: **Web**, **Mail**, **File Transfer**, or **Updates**. To open the CSC SSM GUI, click one of the links in these panes.

Determining What Traffic to Scan

The CSC SSM can scan FTP, HTTP, POP3, and SMTP traffic; however, it supports these protocols only when the destination port of the packet requesting the connection is the established port for the protocol. The CSC SSM can scan only the following connections:

- FTP connections opened to TCP port 21.
- HTTP connections opened to TCP port 80.
- POP3 connections opened to TCP port 110.
- SMTP connections opened to TCP port 25.

You can choose to scan traffic for all of these protocols or any combination of them. For example, if you do not allow network users to receive POP3 e-mail, you would not want to configure the adaptive security appliance to divert POP3 traffic to the CSC SSM. You would want to block POP3 traffic instead.

To maximize performance of the adaptive security appliance and the CSC SSM, divert to the CSC SSM only the traffic that you want the CSC SSM to scan. Diverting traffic that you do not want to scan, such as traffic between a trusted source and destination, can adversely affect network performance.



Note

When traffic is first classified for CSC inspection, it is flow-based. If traffic is part of a pre-existing connection, the traffic goes directly to the policy set for that connection.

You enable traffic scanning with the CSC SSM on the CSC Scan tab in the Add Service Policy Rule Wizard Rule Actions screen. You can apply service policies that include CSC scanning globally or to specific interfaces; therefore, you can choose to enable CSC scans globally or for specific interfaces. For more information, see [Rule Actions for CSC Scanning, page 29-8](#).

Adding the `csc` command to your global policy ensures that all unencrypted connections through the adaptive security appliance are scanned by the CSC SSM; however, this setting may cause traffic from trusted sources to be scanned unnecessarily.

If you enable CSC scans in interface-specific service policies, these scans are bi-directional.

Bi-directional scanning means that when the adaptive security appliance opens a new connection, if CSC scanning is active on either the inbound or the outbound interface of that connection and the service policy identifies traffic for scanning, the adaptive security appliance diverts this traffic to the CSC SSM. Bi-directional scanning also means that if you divert any of the supported traffic types that cross a given interface to the CSC SSM, unnecessary scanning may be occurring on traffic from your trusted inside networks. For example, URLs and files requested from web servers on a DMZ network are unlikely to pose content security risks to hosts on an inside network, and you probably do not want the adaptive security appliance to divert such traffic to the CSC SSM.

Therefore, we highly recommend that the service policies to define CSC scans use access lists to limit the selected traffic. Specifically, use access lists that match the following:

- HTTP connections to outside networks.
- FTP connections from clients inside the adaptive security appliance to servers outside the adaptive security appliance.
- POP3 connections from clients inside the adaptive security appliance to servers outside the adaptive security appliance.
- Incoming SMTP connections destined to go to inside mail servers.

In [Figure 29-3](#), you should configure the adaptive security appliance to divert traffic to CSC SSM requests from clients on the inside network for HTTP, FTP, and POP3 connections to the outside network and incoming SMTP connections from outside hosts to the mail server on the DMZ network. You should not enable scanning of HTTP requests from the inside network to the web server on the DMZ network.

Figure 29-3 Common Network Configuration for CSC SSM Scanning



There are many ways you could configure the adaptive security appliance to identify the traffic that you want to scan. One approach is to define two service policies: one on the inside interface and the other on the outside interface, each with access lists that match traffic to be scanned.

Figure 29-4 shows service policy rules that select only the traffic that the adaptive security appliance should scan.

Figure 29-4 *Optimized Traffic Selection for CSC Scans*



In the inside-policy, the first class, `inside-class1`, ensures that the adaptive security appliance does not scan HTTP traffic between the inside network and the DMZ network. The Match column indicates this setting by displaying the “Do not match” icon. This setting does not mean the adaptive security appliance blocks traffic sent from the 192.168.10.0 network to TCP port 80 on the 192.168.20.0 network. Instead, this setting exempts the traffic from being matched by the service policy applied to the inside interface, which prevents the adaptive security appliance from sending the traffic to the CSC SSM.

The second class of the inside-policy, `inside-class` matches FTP, HTTP, and POP3 traffic between the inside network and any destination. HTTP connections to the DMZ network are exempted because of the `inside-class1` setting. As previously mentioned, policies that apply CSC scanning to a specific interface affect both incoming and outgoing traffic, but by specifying 192.168.10.0 as the source network, `inside-class1` matches only connections initiated by the hosts on the inside network.

In the outside-policy, `outside-class` matches SMTP traffic from any outside source to the DMZ network. This setting protects the SMTP server and inside users who download e-mail from the SMTP server on the DMZ network, without having to scan connections from SMTP clients to the server.

If the web server on the DMZ network receives files uploaded by HTTP from external hosts, you can add a rule to the outside policy that matches HTTP traffic from any source to the DMZ network. Because the policy is applied to the outside interface, the rule would only match connections from HTTP clients outside the adaptive security appliance.

Rule Actions for CSC Scanning

The CSC Scan tab lets you determine whether the CSC SSM scans traffic identified by the current traffic class. This tab appears only if a CSC SSM is installed in the adaptive security appliance.

The CSC SSM scans only HTTP, SMTP, POP3, and FTP traffic. If your service policy includes traffic that supports other protocols in addition to these four, packets for other protocols are passed through the CSC SSM without being scanned. To reduce the load on the CSC SSM, configure the service policy rules that send packets to the CSC SSM to support only HTTP, SMTP, POP3, or FTP traffic.

Fields

- Enable CSC scan for this traffic flow—Enables or disables use of the CSC SSM for this traffic flow. When this check box is checked, the other parameters on this tab become active.

- If CSC card fails—Configures the action to take if the CSC SSM becomes inoperable.
 - Permit traffic—Allows traffic if the CSC SSM fails.
 - Close traffic—Blocks traffic if the CSC SSM fails.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

CSC SSM Setup

The screens under CSC Setup let you configure basic operational parameters for the CSC SSM. You must complete the CSC Setup Wizard at least once before you can configure 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 Home > Trend Micro Content Security > Content Security Tab or Monitoring > Trend Micro Content Security > Content Security Tab 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.

For an introduction to the CSC SSM, see [About the CSC SSM, page 29-2](#). For more information, see the following topics:

- [Activation/License, page 29-10](#)
- [IP Configuration, page 29-11](#)
- [Host/Notification Settings, page 29-11](#)
- [Management Access Host/Networks, page 29-12](#)
- [Password, page 29-13](#)
- [Restoring the Default Password, page 29-14](#)
- [Wizard Setup, page 29-15](#)

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • ¹ | — |

1. In multiple-context mode, the panes under the CSC Setup node are available only in the admin context.

For More Information

See [Managing the CSC SSM, page 29-2](#)

Activation/License

The Activation/License pane lets you configure activation codes for the following two components of the CSC SSM:

- Base License
- 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 page and the CSC UI home page appear at the bottom of this window. The serial number for the assigned license is filled in automatically.

Fields

- Product—*Display only*. Shows the name of the component.
- Activation Code—Contains the activation code for the corresponding Product field.
- License Status—*Display only*. Shows information about the status of the license. If the license is valid, the expiration date appears. If expiration date has passed, this field indicates that the license has expired.
- Nodes—*Display only*. Shows the maximum number of network devices supported by the Base License of your CSC SSM. The Plus License does not affect the number of network devices supported; therefore, the Nodes field does not appear in the Plus License area.
- Click the link provided to review license status or renew your license.
- Click the link provided to go to the CSC home page in ASDM.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • ¹ | — |

1. In multiple-context mode, the Activation/License pane is available only in the admin context.

For More Information

See [Managing the CSC SSM, page 29-2](#)

IP Configuration

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

Fields

- Management Interface—Contains parameters for management access to the CSC SSM.
 - IP Address—Sets the IP address for management access to the CSC SSM.
 - Mask—Sets the netmask for the network containing the management IP address of the CSC SSM.
 - Gateway—Sets the IP address of the gateway device for the network that contains the management IP address of the CSC SSM.
- DNS Servers—Contains parameters about DNS servers for the network containing the management IP address of the CSC SSM.
 - Primary DNS—Sets the IP address of the primary DNS server.
 - Secondary DNS—(Optional) Sets the IP address of the secondary DNS server.
- Proxy Server—Contains parameters for an optional 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, you can leave the fields in this group blank.
 - Proxy Server—(Optional) Sets the IP address of the proxy server.
 - Proxy Port—(Optional) Sets the listening port of the proxy server.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • ¹ | — |

1. In multiple-context mode, the IP Configuration pane is available only in the admin context.

For More Information

See [Managing the CSC SSM, page 29-2](#)

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-mails to be excluded from detailed scanning.

Fields

- **Host and Domain Names**—Contains information about the hostname and domain name of the CSC SSM.
 - **HostName**—Sets the hostname of the CSC SSM.
 - **Domain Name**—Sets the domain name that contains the CSC SSM.
- **Incoming E-mail Domain Name**—Contains information about a trusted incoming e-mail domain name for SMTP-based e-mail.
 - **Incoming Email Domain**—Sets the incoming e-mail domain name. 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 > Email**, 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.

- **Notification Settings**—Contains information required for e-mail notification of events.
 - **Administrator Email**—Sets the e-mail address for the account to which notification e-mails should be sent.
 - **Email Server IP Address**—Sets the IP address of the SMTP server.
 - **Port**—Sets the port to which the SMTP server listens.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • ¹ | — |

1. In multiple-context mode, the Host/Notification Settings pane is available only in the admin context.

For More Information

See [Managing the CSC SSM, page 29-2](#)

Management Access Host/Networks

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

Fields

- **IP Address**—Sets the address of a host or network you want to add to the Selected Hosts/Network list.
- **Mask**—Sets the netmask for the host or network you specified in the IP Address field.
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.
- **Selected Hosts/Networks**—Displays the hosts or networks trusted for management access to the CSC SSM. ASDM requires that you configure at least one host or network. You can configure a maximum of eight hosts or networks.
To remove a host or network from the list, choose its entry in the list and click **Delete**.
- **Add**—Adds the host or network you specified in the IP Address field to the Selected Hosts/Networks list.
- **Delete**—Removes the host or network selected in the Selected Hosts/Networks list.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • 1 | — |

1. In multiple-context mode, the Management Access Host/Networks pane is available only in the admin context.

For More Information

[Managing the CSC SSM, page 29-2](#)

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.”

Fields

- Old Password—Requires the current password for management access to the CSC SSM.
- New Password—Sets the new password for management access to the CSC SSM.
- Confirm New Password—Verifies the new password for management access to the CSC SSM.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • ¹ | — |

1. In multiple-context mode, the Password pane is available only in the admin context.

For More Information

[Managing the CSC SSM, page 29-2](#)

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 session in to the CSC SSM. 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 adaptive 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.

**Note**

This feature is available only in multiple-context mode in the system context.

For More Information

See [Password](#), page 29-13

Wizard Setup

The Wizard Setup screen lets you start the CSC 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 29-15
- [CSC Setup Wizard IP Configuration](#), page 29-16
- [CSC Setup Wizard Host Configuration](#), page 29-17
- [CSC Setup Wizard Management Access Configuration](#), page 29-17
- [CSC Setup Wizard Password Configuration](#), page 29-18
- [CSC Setup Wizard Traffic Selection for CSC Scan](#), page 29-18
- [CSC Setup Wizard Summary](#), page 29-20

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

Fields

- Launch Setup Wizard—Click to start the CSC Setup Wizard.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • ¹ | — |

1. In multiple-context mode, the Wizard Setup screen is available only in the admin context.

For More Information

See [Managing the CSC SSM](#), page 29-2

CSC Setup Wizard Activation Codes Configuration

The CSC Setup Wizard Activation Codes Configuration screen displays the activation codes that you have entered to enable features on the CSC SSM, according to the type of license you have.

Fields

- Activation Code—*Display only*. Displays the activation code settings you have made on this screen.
 - Base License—Shows the activation code. The Base License includes anti-virus, anti-spyware, and file blocking.
 - Plus License—Shows the activation code, if you have entered one. If not, this field is blank. The Plus License includes anti-spam, anti-phishing, content filtering, and URL blocking and filtering.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

CSC Setup Wizard IP Configuration

The CSC Setup Wizard IP Configuration screen displays the IP configuration settings that you have entered for the CSC SSM.

Fields

- IP Address—Shows the IP address for the management interface of the CSC SSM.
- Mask—Shows the network mask for the management interface of the CSC SSM that you have selected from the drop-down list.
- Gateway—Shows the IP address of the gateway device for the network that contains the CSC SSM management interface.
- Primary DNS— Shows the primary DNS server IP address.
- Secondary DNS (optional)—Shows the secondary DNS server IP address (if configured).
- Proxy Server (optional)—Shows the proxy server (if configured).
- Proxy Port (optional)—Shows the proxy port (if configured).

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

CSC Setup Wizard Host Configuration

The CSC Setup Wizard Host Configuration screen displays the host and domain names, incoming e-mail domain name, administrator e-mail address, e-mail server IP address, and the port number that you have entered for the CSC SSM.

Fields

- **Hostname**—Shows the hostname of the CSC SSM.
- **Domain Name**—Shows the name of the domain in which the CSC SSM resides.
- **Incoming Email Domain**—Shows the domain name for incoming e-mail.
- **Administrator E-mail**—Shows the e-mail address of the domain administrator.
- **E-mail Server IP Address**—Shows the IP address of the e-mail server.
- **Port**—Shows the port number through which you connect to the CSC SSM.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM](#)

CSC Setup Wizard Management Access Configuration

The CSC Setup Wizard IP Configuration screen displays the subnet and host settings that you have entered to grant access to the CSC SSM.

Fields

- **IP Address**—Shows the IP address for networks and hosts that are allowed to connect to the CSC SSM.
- **Mask**—Shows 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.
- **Add**—Click to add the IP address of the networks and hosts that you want to allow to connect to the CSC SSM.
- **Delete**—Click to remove the IP address of a network or host whose ability to connect to the CSC SSM you no longer want.
- **Selected Hosts/Networks**—Lists the IP addresses of networks and hosts whose connection to the CSC SSM you have added.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

CSC Setup Wizard Password Configuration

The CSC Setup Wizard Password Configuration screen displays the password settings that you have entered to grant access to the CSC SSM.

Fields

- Old Password—Requires the current password to access the CSC SSM.
- New Password—Sets the new password to access the CSC SSM.
- Confirm New Password—Verifies the new password to access the CSC SSM.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

CSC Setup Wizard Traffic Selection for CSC Scan

The CSC Setup Wizard Traffic Selection for CSC Scan screen displays the settings that you have made to select traffic for CSC scanning.

Fields

- Interface—Specifies the interface to the CSC SSM that you have chosen from the drop-down list.
- Source—Specifies the source of network traffic for the CSC SSM to scan.
- Destination—Specifies the destination of network traffic for the CSC SSM to scan.
- Service—Specifies the source or destination service for the CSC SSM to scan.

- **Add**—Click to specify additional traffic details for CSC scanning. For more information, see [Specify traffic for CSC Scan, page 29-19](#).
- **Edit**—Click to modify additional traffic details for CSC scanning. For more information, see [Specify traffic for CSC Scan, page 29-19](#).
- **Delete**—Click to remove additional traffic details for CSC scanning.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

Specify traffic for CSC Scan

The Specify traffic for CSC Scan dialog box allows you to define, modify, or remove additional settings for selecting traffic for CSC scanning.

Fields

- **Interface**—Choose the type of interface to the CSC SSM from the drop-down list. Available settings are global (all interfaces), inside, management, and outside.
- **Source**—Choose the source of network traffic for the CSC SSM to scan from the drop-down list.
- **Destination**—Choose the destination of network traffic for the CSC SSM to scan from the drop-down list.
- **Service**—Choose the type of service for the CSC SSM to scan from the drop-down list.
- **Description**—Describes the network traffic that you define for the CSC SSM to scan.
- **If CSC card fails**—Specifies whether or not to allow the CSC SSM to scan network traffic if the CSC card fails.

Click **Permit** to allow traffic through without being scanned. Click **Close** to prevent traffic from going through without being scanned. Click **OK** to save your settings. The added traffic details appear on the CSC Setup Wizard Traffic selection for CSC Scan screen. 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.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [CSC Setup Wizard Traffic Selection for CSC Scan, page 29-18](#)

CSC Setup Wizard Summary

The CSC Setup Wizard Summary screen displays the settings that you have made with the CSC Setup Wizard. You can review your selections before you exit the wizard. If you want to change any of the settings, you can click **Back** to return to the previous screens that include those settings, make the needed changes, and click **Next** to return to this screen.



Note After you click **Finish**, you can change any settings related to the CSC SSM without using the CSC Setup Wizard again.

Fields

- Activation Codes—*Display only*. Summarizes the settings that you made in the Activation Codes Configuration screen.
 - Base—Shows the Base License activation code.
 - Plus—Shows the Plus License activation code, if you entered one. If not, this field is blank.
- IP Parameters—*Display only*. Summarizes 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).
- Host and Domain Names—*Display only*. Summarizes 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.
- Management Access List—Summarizes the settings that you have made on the Management Access Configuration screen. The drop-down list includes the hosts and networks from which the CSC SSM will allow management connections.

- Password—*Display only*. Indicates whether or not you have changed the password in the Password Configuration screen.
- Back—Click to return to preceding screens of the CSC Setup Wizard.
- Next—Dimmed; however, if you click **Back** to access any of the preceding screens in this wizard, click **Next** to return to this screen.
- Finish—Completes the CSC Setup Wizard and saves all settings that you have specified.
- Cancel—Exits the CSC Setup Wizard without saving any of the selected settings. If you click **Cancel**, ASDM displays a dialog box to confirm your decision.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

Web

The Web pane lets you view whether or not web-related features are enabled and lets you access the CSC SSM for configuring these 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.

Fields

- URL Blocking and Filtering—Includes information and links related to URL blocking and filtering.
 - URL Blocking—*Display only*. Shows whether or not URL blocking is enabled on the CSC SSM.
 - Configure URL Blocking—Opens a screen for configuring URL blocking on the CSC SSM.
 - URL Filtering—*Display only*. Shows whether or not URL filtering is enabled on the CSC SSM.
 - Configure URL Filtering Rules—Opens a screen for configuring URL filtering rules on the CSC SSM.
 - Configure URL Filtering Settings—Opens a screen for configuring settings for URL filtering on the CSC SSM.
- File Blocking—Includes a field and a link about HTTP file blocking on the CSC SSM.
 - File Blocking—*Display only*. Shows whether or not file blocking is enabled on the CSC SSM.
 - Configure File Blocking—Opens a screen for configuring HTTP file blocking settings on the CSC SSM.

- Scanning—Includes a field and a link about HTTP scanning on the CSC SSM.
 - HTTP Scanning—*Display only*. Shows whether or not HTTP scanning is enabled on the CSC SSM.
 - Configure Web Scanning—Opens a screen for configuring HTTP scanning on the CSC SSM.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

Mail

The Mail pane lets you see whether or not e-mail-related features are enabled and lets you access the CSC SSM to configure these features.

For more information about configuring these areas, see the following topics:

- [SMTP Tab, page 29-22](#)
- [POP3 Tab, page 29-23](#)

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

SMTP Tab

The SMTP tab displays fields and links specific to SMTP e-mail features on the CSC SSM.



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.

Fields

- Scanning—Includes fields and links about SMTP scanning.
 - Incoming Scan—*Display only*. Shows whether or not the incoming SMTP scanning feature is enabled on the CSC SSM.
 - Configure Incoming Scan—Opens a screen for configuring incoming SMTP scan settings on the CSC SSM.
 - Outgoing Scan—*Display only*. Shows whether or not the outgoing SMTP scanning feature is enabled on the CSC SSM.
 - Configure Outgoing Scan—Opens a screen for configuring outgoing SMTP scan settings on the CSC SSM.
- Content Filtering—Includes fields and links about SMTP content filtering.
 - Incoming Filtering—*Display only*. Shows whether or not content filtering for incoming SMTP e-mail is enabled on the CSC SSM.
 - Configure Incoming Filtering—Opens a screen for configuring incoming SMTP content filtering settings on the CSC SSM.
 - Outgoing Filtering—*Display only*. Shows whether or not content filtering for outgoing SMTP e-mail is enabled on the CSC SSM.
 - Configure Outgoing Filtering—Opens a screen for configuring outgoing SMTP content filtering settings on the CSC SSM.
- Anti-spam—Includes fields and links about the SMTP anti-spam feature.
 - Spam Prevention—*Display only*. Shows whether or not the SMTP anti-spam feature is enabled on the CSC SSM.
 - Configure Anti-spam—Opens a screen for configuring SMTP anti-spam settings on the CSC SSM.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

POP3 Tab

The POP3 tab displays fields and links specific to POP3 e-mail features on the CSC SSM.

**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.

Fields

- Scanning—*Display only*. Shows whether or not POP3 e-mail scanning is enabled on the CSC SSM.
- Configure Scanning—Opens a screen for configuring POP3 e-mail scanning on the CSC SSM.
- Anti-spam—*Display only*. Shows whether or not the POP3 anti-spam feature is enabled on the CSC SSM.
- Configure Anti-spam—Opens a screen for configuring the POP3 anti-spam feature on the CSC SSM.
- Content Filtering—*Display only*. Shows whether or not POP3 e-mail content filtering is enabled on the CSC SSM.
- Configure Content Filtering—Opens a screen for configuring POP3 e-mail content filtering on the CSC SSM.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

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.

Fields

- File Scanning—*Display only*. Shows whether or not FTP file scanning is enabled on the CSC SSM.
- Configure File Scanning—Opens a screen for configuring FTP file scanning settings on the CSC SSM.
- File Blocking—*Display only*. Shows whether or not FTP file blocking is enabled on the CSC SSM.

- Configure File Blocking—Opens a screen for configuring FTP file blocking settings on the CSC SSM.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)

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.

Fields

- Scheduled Updates—*Display only*. Shows whether or not scheduled updates are enabled on the CSC SSM.
- Scheduled Update Frequency—Displays information about when updates are scheduled to occur, such as “Hourly at 10 minutes past the hour.”
- Component—Displays names of parts of the CSC SSM software that can be updated.
- Scheduled Updates—*Display only*. Shows whether or not scheduled updates are enabled for the corresponding components.
- Configure Updates—Opens a window for configuring scheduled update settings on the CSC SSM.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

For More Information

See [Managing the CSC SSM, page 29-2](#)