



## CHAPTER 35

# Configuring Trend Micro Content Security

---

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.

## Managing the CSC SSM

This section contains the following topics:

- [About the CSC SSM, page 35-1](#)
- [Getting Started with the CSC SSM, page 35-3](#)
- [Determining What Traffic to Scan, page 35-5](#)

## About the CSC SSM

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 35-1](#) 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 what 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 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.



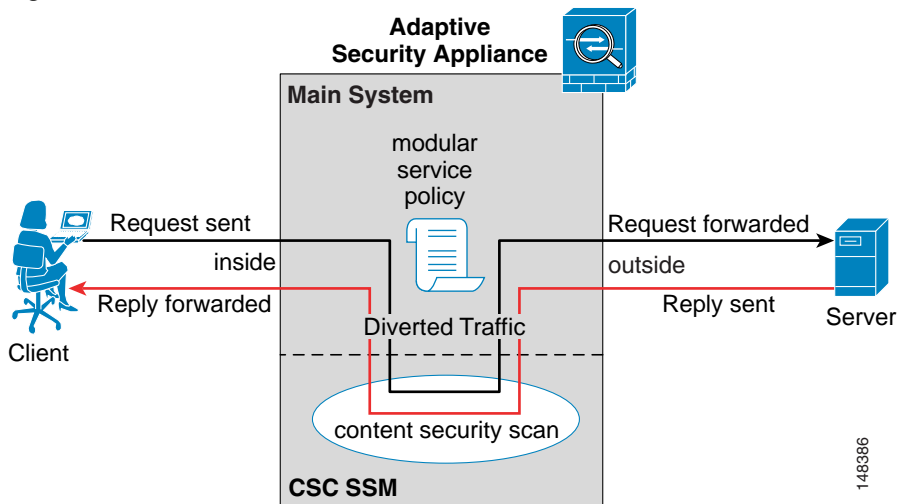
**Note**

---

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 35-1 Flow of Scanned Traffic with CSC SSM



You use ASDM for system setup and monitoring of the CSC SSM. For advanced configuration of content security policies in the CSC SSM software, you access the web-based GUI for the CSC SSM by clicking links within ASDM. The CSC SSM GUI appears in a separate web browser, which may prompt you for the CSC SSM password. Use of the CSC SSM GUI is explained in the *Cisco Content Security and Control SSM Administrator Guide*.



**Note**

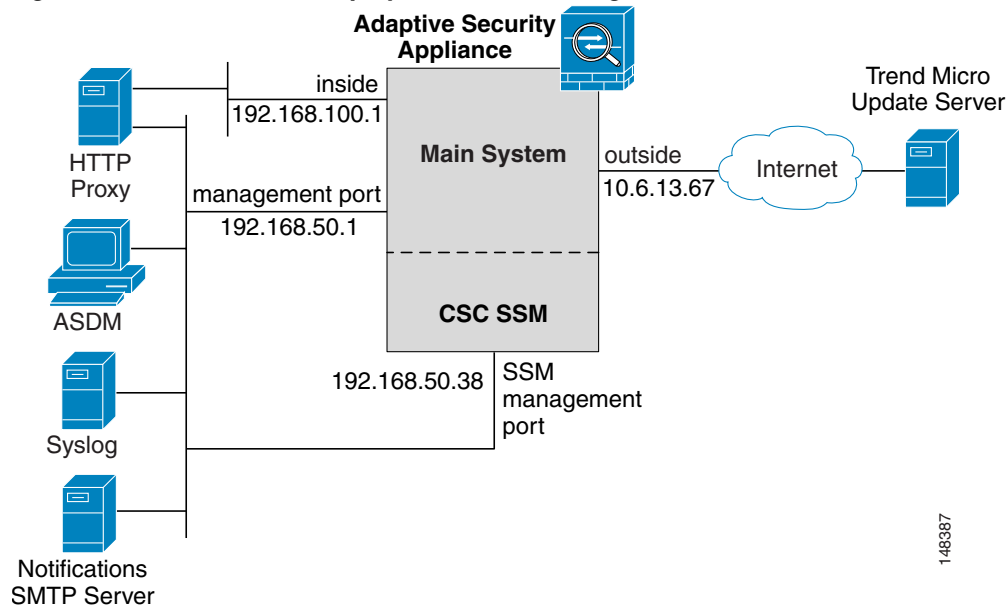
ASDM and the CSC SSM maintain separate passwords. You can configure their passwords to be identical; however, changing one of these two passwords does not affect the other password.

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 35-2 shows an adaptive security appliance with a CSC SSM that is connected to a dedicated management network. While use of a dedicated management network is not required, we recommend it. Of particular interest in Figure 35-2 are the following:

- An HTTP proxy server is connected to the inside network and to the management network. This enables 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 permit 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 35-2 CSC SSM Deployment with a Management Network



146387

## Getting Started with the CSC SSM

Before you receive the security benefits provided by a CSC SSM, you must perform several steps beyond simple hardware installation of the SSM. This procedure provides an overview of those steps.

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

- 
- Step 1** If the CSC SSM did not come pre-installed in a Cisco ASA 5500 series adaptive security appliance, install it and connect a network cable to the management port of the SSM. For assistance with installation and connecting the SSM, see the *Cisco ASA 5500 Series Getting Started Guide*.
- The management port of the CSC SSM 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 syslogging.
- Step 2** With the CSC SSM, you should have 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** Gather the following information, for use in [Step 5](#).
- Activation keys, received after completing [Step 2](#).
  - 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 (required 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 allowed to manage the CSC SSM.
- Password for the CSC SSM.

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

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

**Step 5** Run the CSC Setup Wizard.

- If you have not run the CSC Setup Wizard, choose **Configuration > Trend Micro Content Security** and the Setup Wizard starts automatically.
- If you are rerunning the Setup Wizard, choose **Configuration > Trend Micro Content Security**, connect to and log into the CSC SSM, choose **CSC Setup > Wizard Setup**, and click **Launch Wizard Setup**.

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

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

If you create a global service 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 only traffic from untrusted sources.

For a discussion of best practices for diverting traffic to the CSC SSM, see [Determining What Traffic to Scan](#).

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

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

The adaptive security appliance begins diverting traffic to the CSC SSM, which performs the content security scans enabled by the license 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 is advanced configuration that you should perform only after reading the *Cisco Content Security and Control SSM Administrator Guide*.

You review the content security policies by viewing the enabled features in the CSC SSM GUI. The availability of features depends on the license level you purchased. By default, all features included in the license 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 select one of the following: **Web**, **Mail**, **File Transfer**, or **Updates**. The blue links on these panes, beginning with the word “Configure”, open the CSC SSM GUI.

---

## Determining What Traffic to Scan

The CSC SSM can scan FTP, HTTP, POP3, and SMTP traffic. It supports these protocols only when the destination port of the packet requesting the connection is the well known port for the protocol, that is, 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 it 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. Needlessly diverting traffic that you do not want to scan, such as traffic between a trusted source and destination, can adversely affect network performance.

The action of scanning traffic with the CSC SSM is enabled on the CSC Scan tab of the Add Service Policy Rule Wizard—Rule Actions window. Service policies that include a CSC scan action can be applied globally or to specific interfaces; therefore, you can choose to enable CSC scans globally or for specific interfaces.

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 may mean that traffic from trusted sources is needlessly scanned.

If you enable CSC scans in interface-specific service policies, they are bi-directional. This means that when the adaptive security appliance opens a new connection, if a CSC scan action is active on either the inbound or the outbound interface of the connection and if the service policy identifies traffic for scanning, the adaptive security appliance diverts this traffic to the CSC SSM.

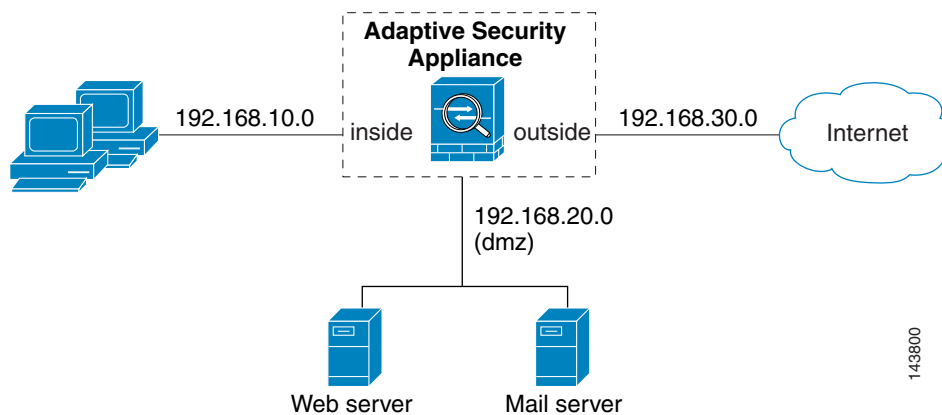
However, bi-directionality means that if you divert any of the supported traffic types that cross a given interface to the CSC SSM, it is likely performing needless scans on traffic from your trusted inside networks. For example, URLs and files requested from web servers on a DMZ network are unlikely 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 defining CSC scans use access lists to limit the traffic selected. 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 inside mail servers.

In [Figure 35-3](#), the adaptive security appliance should be configured 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. HTTP requests from the inside network to the web server on the DMZ network should not be scanned.

**Figure 35-3** 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 35-4](#) shows service policy rules that select only the traffic that should be scanned.

Figure 35-4 Optimized Traffic Selection for CSC Scans

Traffic Classification								Rule Actions
#	Name	Enabled	Match	Source	Destination	Service	Time	
Interface: inside, Policy: inside-policy								
1	inside-class1	<input checked="" type="checkbox"/>		192.168.10.0/24	192.168.20.0/24	www/tcp	-- Not Appl...	csc , permit traffic
1	inside-class	<input checked="" type="checkbox"/>		192.168.10.0/24	any	ftp/tcp	-- Not Appl...	csc , permit traffic
2		<input checked="" type="checkbox"/>		192.168.10.0/24	any	www/tcp	-- Not Appl...	
3		<input checked="" type="checkbox"/>		192.168.10.0/24	any	pop3/tcp	-- Not Appl...	
Interface: outside, Policy: outside-policy								
1	outside-class	<input checked="" type="checkbox"/>		any	192.168.20.0/24	smtp/tcp	-- Not Appl...	csc , permit traffic

In the inside-policy, the first class, `inside-class1`, ensures that HTTP traffic between the inside network and the DMZ network is not scanned. The Match column indicates this by displaying the “Do not match” icon. This 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. It simply exempts the traffic from being matched by the service policy applied to the inside interface and thus 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 due to `inside-class1`. As previously mentioned, policies applying a CSC scan action to a specific interface are effective on both ingress and egress 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 protects the SMTP server and thus protects 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 could 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.

## CSC Setup

The panes under CSC Setup let you configure basic operational parameters for the CSC SSM. You must complete the Setup Wizard once before you can configure each pane separately. After you complete the Setup Wizard, you can modify each pane individually without using the Setup Wizard again.

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

For an introduction to CSC SSM, see [About the CSC SSM](#).

- [Activation/License](#)

- [IP Configuration](#)
- [Host/Notification Settings](#)
- [Management Access Host/Networks](#)
- [Password](#)
- [Restoring the Default Password](#)
- [Wizard Setup](#)
- [Summary](#)

### Modes

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

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	• <sup>1</sup>	—

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

### For More Information

[Managing the CSC SSM](#)

## 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.

### 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.

### Modes

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

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	• <sup>1</sup>	—

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

### For More Information

[Managing the CSC SSM](#)

## 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 for the gateway device. This is the gateway device for the network containing 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—(Optional) 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 boxes in this group empty.
  - 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
•	•	•	• <sup>1</sup>	—

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

**For More Information**[Managing the CSC SSM](#)

## 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 messages 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 depends upon the license 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 click one of the links to access the CSC SSM. After logging in to the CSC SSM, choose **Mail (SMTP) > Configuration**, and click the **Incoming Mail** tab.

- Notification Settings—Contains information required for e-mail notification of events.
  - Administrator E-mail—Sets the e-mail address for the account to which e-mail notification should be sent.
  - E-mail 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
•	•	•	• <sup>1</sup>	—

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

**For More Information**[Managing the CSC SSM](#)

## 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 to the Selected Hosts/Networks list the host or network you specified in the IP Address field.
- **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](#)

## 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, but 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. Because of this, ASDM displays a confirmation dialog box before changing the password.

**Tip**

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

**Note**

The default password is “cisco.”

Passwords appear as asterisks when you type them.

Passwords must be 5 - 32 characters long.

**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
•	•	•	• <sup>1</sup>	—

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

**For More Information**

[Managing the CSC SSM](#)

## Restoring the Default Password

Tools > CSC Password Reset

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).

**Note**

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

To reset the CSC SSM password to the default, 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.

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 7.2(2) or later on the adaptive security appliance and the most recent Version 6.1 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**

[Password](#)

## Wizard Setup

The Wizard Setup pane lets you start the Setup Wizard.

Before you can directly access any of the other panes under CSC Setup, you must complete the Setup Wizard.

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

**Fields**

- Launch Setup Wizard—Starts the CSC SSM 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
•	•	•	• <sup>1</sup>	—

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

**For More Information**

[Managing the CSC SSM](#)

## Summary

The Summary pane displays the results of your actions while using the CSC Setup Wizard. The Summary pane lets you check your work before you exit the wizard. If you want to change any of the settings, you can click < **Back** to return to the panes containing those settings, make the needed changes, and click **Next** > to return to the Summary pane.

**Note**

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

**Fields**

- Activation Codes—*Display only*. Summarizes the settings you made on the Activation Codes Configuration pane.
  - 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 you made on the IP Configuration pane, including the following information:
  - IP address and netmask for the management interface of the CSC SSM.
  - IP address of the gateway device for the networking containing 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 you made on the Host Configuration pane, including the following information:
  - Hostname of the CSC SSM.
  - Domain name for the domain containing the CSC SSM.
  - Domain name for incoming e-mail.
  - Administrator e-mail address.
  - E-mail server IP address and port number.
- Management Access List—*Display only*. Summarizes the settings you made on the Management Access Configuration pane. The drop-down list contains the hosts and networks from which the CSC SSM will allow management connections.
- Password—*Display only*. Indicates whether you changed the password on the Password Configuration pane.
- < Back—Lets you go to preceding panes of the CSC Setup Wizard.
- Next >—On the Summary pane, this button is dimmed; however, if you use Back > to access any of the preceding panes in the wizard, clicking this button returns you to the Summary pane.
- Finish—Completes the CSC Setup Wizard and saves all the settings you made while using the wizard.
- Cancel—Exits the CSC Setup Wizard without saving any of the settings you made. 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**

[Managing the CSC SSM](#)

## Web

The Web pane lets you view whether web-related features are enabled and lets you access the CSC SSM for configuring web-related features.

**Note**

Accessing the CSC SSM requires the CSC SSM password, for which the browser displaying the CSC SSM GUI prompts you. Sessions in the CSC SSM browser window 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 because one session is already open.

**Fields**

- URL Blocking And Filtering—Contains information and links related to URL blocking and filtering.
  - URL Blocking—*Display only*. Shows whether the URL Blocking feature is enabled on the CSC SSM.
  - Configure URL Blocking—Opens a window for configuring URL blocking on the CSC SSM.
  - URL Filtering—*Display only*. Shows whether the URL Filtering feature is enabled on the CSC SSM.
  - Configure URL Filtering Rules—Opens a window for configuring URL filtering rules on the CSC SSM.
  - Configure URL Filtering Settings—Opens a window for configuring settings for URL filtering on the CSC SSM.
- File Blocking—Contains a field and a link about the HTTP file blocking feature on the CSC SSM.
  - File Blocking—*Display only*. Shows whether the file blocking feature is enabled on the CSC SSM.
  - Configure File Blocking—Opens a window for configuring HTTP file blocking settings on the CSC SSM.
- Scanning—Contains a field and a link about the HTTP scanning feature on the CSC SSM.
  - HTTP Scanning—*Display only*. Shows whether the HTTP scanning feature is enabled on the CSC SSM.
  - Configure Web Scanning—Opens a window 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**

[Managing the CSC SSM](#)

## Mail

The Mail pane lets you see if e-mail-related features are enabled and lets you access the CSC SSM for configuring these features.

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

- [Mail > SMTP Tab](#)
- [Mail > POP3 Tab](#)

**Modes**

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

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

## Mail > SMTP Tab

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

**Note**

Accessing the CSC SSM requires the CSC SSM password, for which the browser displaying the CSC SSM GUI prompts you. Sessions in the CSC SSM browser window 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 because one session is already open.

**Fields**

- Scanning—Contains fields and links about SMTP scanning.
  - Incoming Scan—*Display only*. Shows whether the incoming SMTP scanning feature is enabled on the CSC SSM.
  - Configure Incoming Scan—Opens a window for configuring incoming SMTP scan settings on the CSC SSM.

- Outgoing Scan—*Display only*. Shows whether the outgoing SMTP scanning feature is enabled on the CSC SSM.
- Configure Outgoing Scan—Opens a window for configuring outgoing SMTP scan settings on the CSC SSM.
- Content Filtering—Contains fields and links about SMTP content filtering.
  - Incoming Filtering—*Display only*. Shows whether content filtering for incoming SMTP e-mail is enabled on the CSC SSM.
  - Configure Incoming Filtering—Opens a window for configuring incoming SMTP content filtering settings on the CSC SSM.
  - Outgoing Filtering—*Display only*. Shows whether content filtering for outgoing SMTP e-mail is enabled on the CSC SSM.
  - Configure Outgoing Filtering—Opens a window for configuring outgoing SMTP content filtering settings on the CSC SSM.
- Anti-spam—Contains fields and links about the SMTP anti-spam feature.
  - Spam Prevention—*Display only*. Shows whether the SMTP anti-spam feature is enabled on the CSC SSM.
  - Configure Anti-spam—Opens a window 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

[Managing the CSC SSM](#)

## Mail > POP3 Tab

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



### Note

Accessing the CSC SSM requires the CSC SSM password, for which the browser displaying the CSC SSM GUI prompts you. Sessions in the CSC SSM browser window 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 because one session is already open.

### Fields

- Scanning—*Display only*. Shows whether the POP3 e-mail scanning feature is enabled on the CSC SSM.
- Configure Scanning—Opens a window for configuring POP3 e-mail scanning on the CSC SSM.

- Anti-spam—*Display only*. Shows whether the POP3 anti-spam feature is enabled on the CSC SSM.
- Configure Anti-spam—Opens a window for configuring the POP3 anti-spam feature on the CSC SSM.
- Content Filtering—*Display only*. Shows whether POP3 e-mail content filtering is enabled on the CSC SSM.
- Configure Content Filtering—Opens a window 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

[Managing the CSC SSM](#)

## File Transfer

The File Transfer pane lets you view whether FTP-related features are enabled and lets you access the CSC SSM for configuring FTP-related features.



### Note

Accessing the CSC SSM requires the CSC SSM password, for which the browser displaying the CSC SSM GUI prompts you. Sessions in the CSC SSM browser window timeout 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 because one session is already open.

### Fields

- File Scanning—*Display only*. Shows whether the FTP file scanning feature is enabled on the CSC SSM.
- Configure File Scanning—Opens a window for configuring FTP file scanning settings on the CSC SSM.
- File Blocking—*Display only*. Shows whether the FTP file blocking feature is enabled on the CSC SSM.
- Configure File Blocking—Opens a window 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**

[Managing the CSC SSM](#)

## Updates

The Updates pane lets you view whether scheduled updates are enabled and lets you access the CSC SSM for configuring scheduled updates.

**Note**

Accessing the CSC SSM requires the CSC SSM password, for which the browser displaying the CSC SSM GUI prompts you. Sessions in the CSC SSM browser window 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 because one session is already open.

**Fields**

- Scheduled Updates—*Display only*. Shows whether 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 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**

[Managing the CSC SSM](#)

# Connecting to CSC/Content Security and Control Password

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 them to be identical, but changing the CSC SSM password does not affect the ASDM password.

## Fields

- **Connecting to CSC**—Lets you specify the IP address for the management port on the CSC 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.
  - **Management IP Address**—Sets the management IP address for the connection to the CSC SSM to an IP address detected by ASDM. This is the default selection.
  - **Other IP Address or Hostname**—Sets the management IP address to the value you enter.
- **CSC Password**—Lets you specify the password for accessing the CSC SSM. Providing the password enables ASDM to establish a connection to the CSC SSM. It uses the connection to retrieve monitoring and status information, including information about the features enabled on the CSC SSM.

For ten minutes after you have entered the password, clicking links that open the CSC SSM GUI does not require that you reenter the CSC SSM password in the browser that displays the CSC SSM GUI.

- **Password**—Requires the CSC SSM password. If you have not completed the Setup Wizard at Configuration > Trend Micro Content Security > CSC Setup, use the default CSC password. Then complete the configuration in the Setup Wizard, which includes changing the default password.



## Note

The default CSC SSM password is “cisco.”

## 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

[Managing the CSC SSM](#)