Introducing the CSC SSM

This chapter introduces the Content Security and Control (CSC) Security Services Module (SSM), and includes the following sections:

Overview

Trend Micro InterScan for Cisco CSC SSM provides an all-in-one antivirus and spyware management solution for your network. This guide describes how to manage the CSC SSM, which resides in your adaptive security appliance, to do the following:

- Detect and take action on viruses, worms, Trojans, and other threats in your SMTP, POP3, HTTP, and FTP network traffic.

Note The CSC SSM does not scan traffic using other protocols, such as HTTPS.

- Block compressed or very large files that exceed specified parameters.
- Scan for and remove spyware, adware, and other types of grayware.

These features are available to all customers with the Base License for the CSC SSM software. If you have purchased the Plus level of the CSC SSM license in addition to the Base License, you can also:

- Reduce spam and protect against phishing fraud in SMTP and POP3 traffic.
- Set up content filters to allow or prohibit e-mail traffic containing key words or phrases.
- Block URLs that you do not want employees to access, or URLs that are known to have hidden or malicious purposes.

- Filter URL traffic according to predefined categories that you allow or disallow, such as adult or mature content, games, chat or instant messaging, or gambling sites.

For more information about the Base License and Plus License, see the "Licensing" section on page 1-10.

To start scanning traffic, you must create one or more service policy rules to send traffic to the CSC SSM for scanning. See the ASA 5500 series adaptive security appliance documentation for information about how to create service policy rules using the command line or using ASDM.

With Trend Micro InterScan for Cisco CSC SSM, you do not need to install separate applications for virus protection, spyware blocking, spam detection, or content filtering—all of these functions are available in a single, easy-to-maintain package. Trend Micro InterScan for Cisco CSC SSM provides protection for major traffic protocols—SMTP, HTTP, and FTP, as well as POP3 traffic, to ensure that employees do not accidentally introduce viruses from their personal e-mail accounts.

For information about installing the appliance, see your Cisco documentation.

This guide familiarizes you with the Trend Micro InterScan for Cisco CSC SSM user interface, and describes configuration settings that you may want to fine-tune after installation. For a description of fields in a specific window, see the CSC SSM online help.

Features and Benefits

Trend Micro InterScan for Cisco CSC SSM helps you manage threats to your network. Table 1-1 provides an overview of the features and benefits:

Table 1-1 Features and Benefits

Features	Benefits
Scans for traffic containing viruses, and manages infected messages and files.	Together with powerful Cisco firewall protection, Trend Micro InterScan for Cisco CSC SSM secures your network from threats, spam, and unwanted content.
Scans for spam at low to high threshold levels, and allows you to determine how spam is handled.	Easy to install, with a Setup Wizard.

Table 1-1 Features and Benefits (continued)

Features	Benefits
Filters offensive or inappropriate content.	Antivirus, spyware and grayware detection, file blocking, and other protections against security risks in your network traffic are integrated with ASDM.
Blocks incoming file types that can damage your network.	
Helps prevent Denial of Service attacks by setting limits on message size.	
Provides approved senders and blocked senders functionality for file and URL blocking.	
Filters access to URLs by category.	
Blocks connections to URLs or FTP sites prohibited by your corporate policies.	
Allows you to fine-tune configuration of scanning, anti-spam, and filtering features after installation.	
Can be configured to update the virus pattern file, scan engine, and spam-detection components automatically when a new version becomes available from Trend Micro.	
Provides e-mail and system log message notifications to make sure you stay informed of activity.	
Provides log files that are purged automatically after 30 days.	
Provides a user-friendly console that includes online help to guide you through tasks.	
Automatically displays a notification when your license is about to expire.	

Available Documentation

The documentation for this product assumes that you are a system administrator who is familiar with the basic concepts of managing firewalls and administering a network. It is also assumed that you have privileges to manage the security applications in your network.

Before proceeding, you might also want to read *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*. This guide includes documentation for installing the CSC SSM if the appliance you purchased does not have the SSM already installed.

The documentation available for Trend Micro InterScan for Cisco CSC SSM includes the following:

- This document—*Cisco Content Security and Control SSM Administrator Guide*
- Online Help—Two types of online help are available:
  - Context-sensitive window help, which explains how to perform tasks in one window.
  - General help, which explains tasks that require action in several windows, or additional knowledge needed to complete tasks.

- Knowledge Base—An online database of problem-solving and troubleshooting information. Knowledge Base provides the most current information about known product issues. To access the Knowledge Base, go to the following URL:

  kb.trendmicro.com/solutions/solutionSearch.asp

Terminology

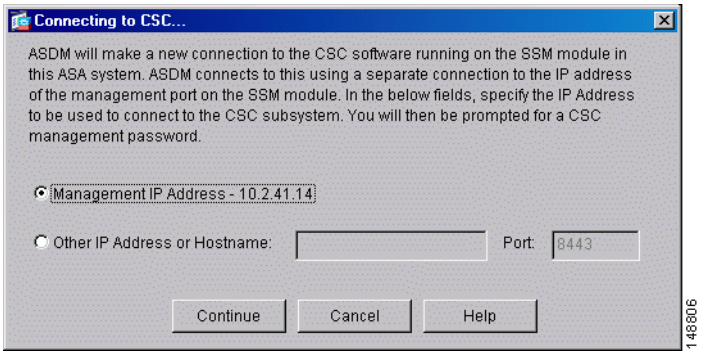
Certain terms are used throughout the documentation and online help that may not be familiar to you, or may be used in an alternate way from what you might expect. A definition of terms is available in the Glossary.

Introducing the Content Security Tab

When you open ASDM, the ASA Main System tab is the default view. Click the **Content Security** tab to view a summary of CSC SSM activities.

You are prompted to connect to the CSC SSM. The Connecting to CSC dialog box appears (shown in Figure 1-1), in which you choose the IP address that ASDM recognizes, or an alternate. You can use an alternate if you access ASDM through a NAT device, in which the IP address of the CSC SSM that is visible from your computer is different from the actual IP address of the CSC SSM management port.

Figure 1-1 Connecting to the CSC



Click **Continue** after choosing the local host or the alternate.

Enter your CSC SSM password, which you configured during installation, and click **OK**.

The Content Security tab appears. For more information, see Features of the Content Security Tab, page 7-1.

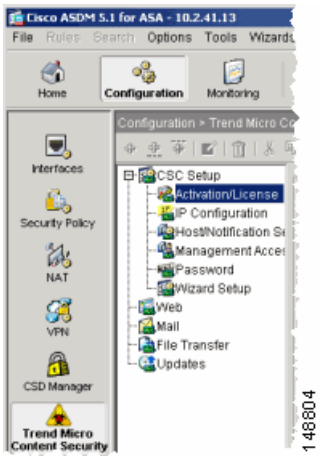
Configuring Content Security

To open the CSC SSM, choose **Configuration > Trend Micro Content Security.** From the Configuration menu (shown in Figure 1-2), select from the following configuration options:

- CSC Setup—Launches the Setup Wizard to install and configure the CSC SSM.
- Web—Configures Web scanning, file blocking, URL filtering, and URL blocking.

- Mail—Configures scanning, content filtering, and spam prevention for incoming and outgoing SMTP and POP3 e-mail.
- File Transfer—Configures file scanning and blocking.
- Updates—Schedules updates for content security scanning components (virus pattern file, scan engine, and others).

Figure 1-2 Configuration Options on ASDM



The Setup options are described in the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*. The online help provides more detailed information about each of these options.

The Web, Mail, File Transfer, and Updates options are described in more detail in these chapters:

- Mail—Chapter 3, "Configuring SMTP and POP3 Mail Traffic."
- Web and File Transfer—Chapter 4, "Configuring Web (HTTP) and File Transfer (FTP) Traffic."
- Updates—Chapter 5, "Managing Updates and Log Queries."

Introducing the CSC SSM Console

This section describes the CSC SSM console, and includes the following topics:

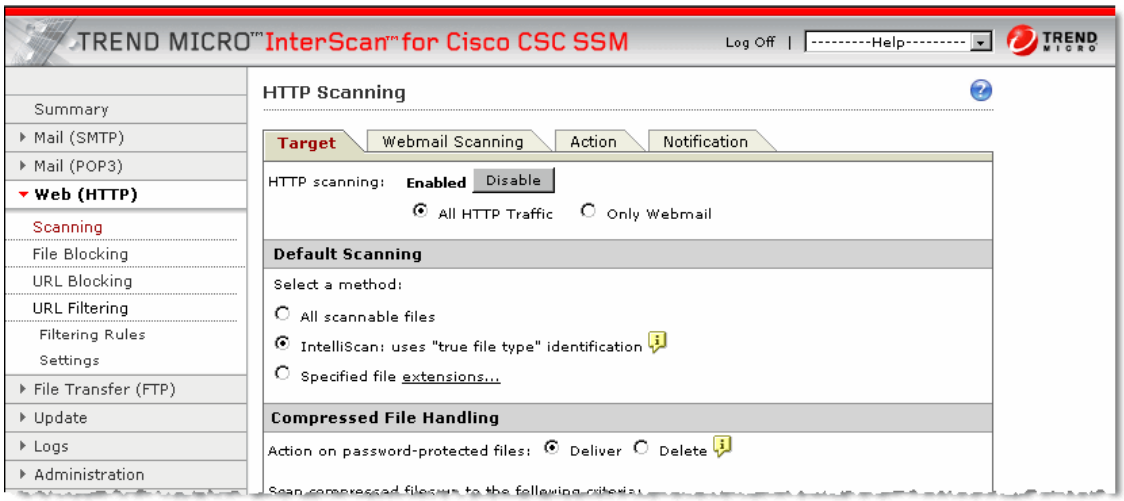
After you have successfully installed Trend Micro InterScan for Cisco CSC SSM and have configured the adaptive security appliance to send traffic to CSC SSM, the virus scanning and detection feature is activated and your network traffic is scanned according to the default settings. Additional features, such as spyware or grayware detection, are not enabled by default and you must configure them in the CSC SSM.

The CSC SSM displays in a browser window, as shown in Figure 1-3. On the left side of the Configuration window in ASDM are links to perform the tasks of interest. The default view in the Trend Micro InterScan for Cisco CSC SSM is context-sensitive, depending on the link selected. For example, click the **Configure Web Scanning** link to go to the HTTP Scanning window, where you can configure Web scanning settings.

The first time you log in to the CSC SSM, ASDM displays a security certificate, followed by the Connecting to CSC <link name> window. If you exit the CSC SSM and then return without logging out of ASDM, only the security certificate appears.

To exit the application, click **Log Off**, and then close the browser window.

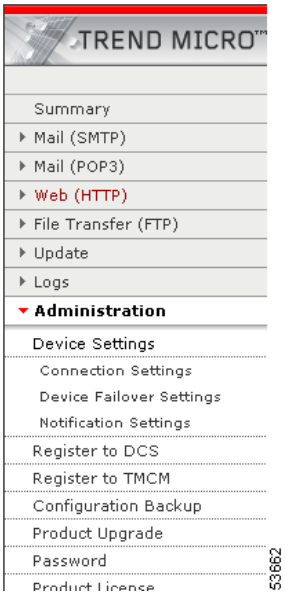
Figure 1-3 HTTP Scanning Window



Navigation Pane

The left pane of the Trend Micro CSC SSM console is the main menu, which also serves as a navigation pane (shown in Figure 1-4). Click a menu item in the navigation pane to open the corresponding window. A selection is compressed when the arrow is pointing to the right; a selection is expanded when the arrow is pointing down. The corresponding panes do not refresh until you choose a selection on the main menu.

Figure 1-4 Navigation Pane in the Trend Micro CSC SSM Console

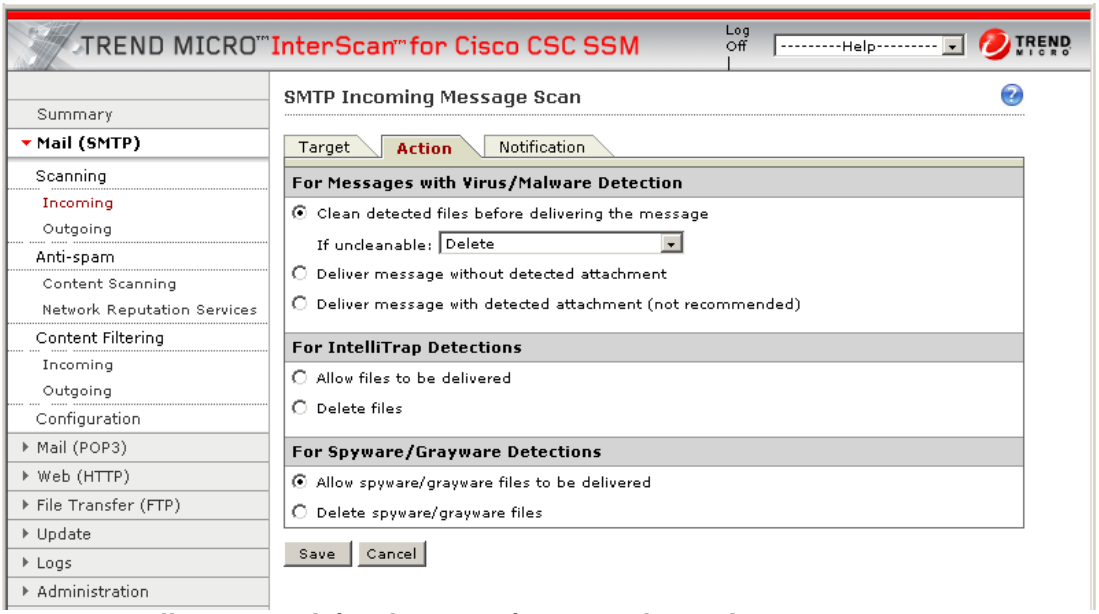


Tab Behavior

The interactive windows for your selection appear on the right side of the CSC SSM console. Most windows in the user interface have multiple views. For example, the SMTP Incoming Message Scan window has three views: Target, Action, and Notification. You can switch among views by clicking the appropriate tab for the information you want. The active tab name appears in brown text; inactive tab names appear in black text.

Typically the tabs are related and work together. For example, in Figure 1-5, you need to use all three tabs to configure virus scanning of incoming SMTP traffic.

Figure 1-5 Tabs Working Together



- Target—Allows you to define the scope of activity to be acted upon.
- Action—Allows you to define the action to be taken when a threat is detected—examples of actions are clean or delete.
- Notification—Allows you to compose a notification message, as well as define who is notified of the event and the action.

For related tabs, you can click **Save** once to retain work on all three tabs.

Save Button

The Save button is disabled when the window first opens. After you perform tasks, the text on the button appears black instead of gray. This is an indication that you must click the button to retain the work you have done.

Default Values

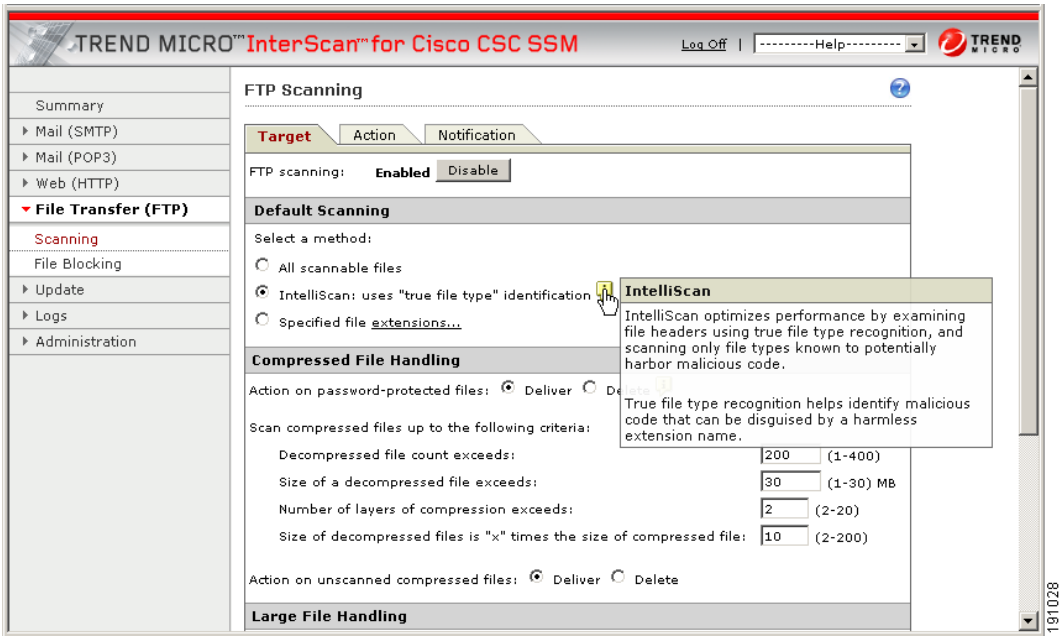
Many windows in the Trend Micro for Cisco CSC SSM user interface include fields that contain default selections. A default selection represents the choice that is best for most users, but you may change the default if another choice is better for your environment. For more information about entries in a particular field, see the online help.

Fields that allow you to compose a notification contain a default message. You can change default notifications by editing or replacing the existing entry.

Tooltips

Some windows on the CSC SSM console contain information called a tooltip. Place your mouse over an icon to display a pop-up text box with additional information that helps you make a decision or complete a task. In the following example (shown in Figure 1-6), positioning the mouse over an icon displays more information about IntelliScan, one of several virus scanning options.

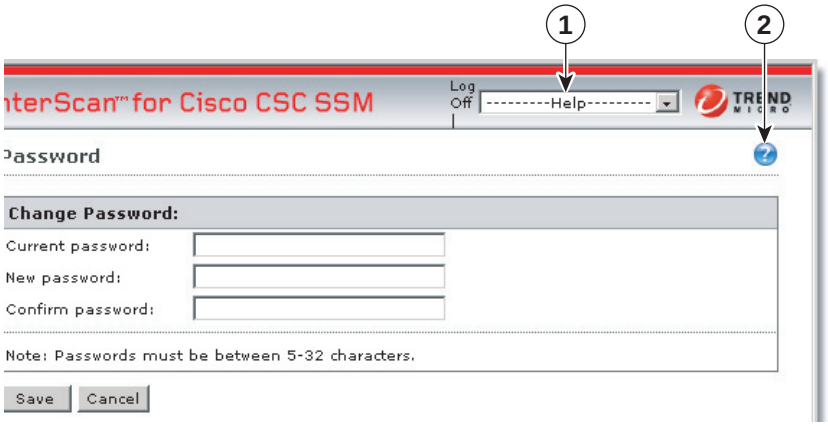
Figure 1-6 Tooltip Example



Online Help

Figure 1-7 shows the two types of online help available with Trend Micro InterScan for Cisco CSC SSM: general help from the Help drop-down menu (1) and context-sensitive help from the Help icon (2).

Figure 1-7 General and Context-sensitive Online Help



To open general help, click the **Contents** and **Index** entry from the Help drop-down menu. A second browser window opens, which allows you to view the help contents shown in Figure 1-8. Click the **plus** sign to expand a help topic.

Figure 1-8 Online Help Contents

After an introduction, the organization of the online help topics follows the structure of the menu on the left in the user interface. Additional information about computer viruses is also available.

To view the online help index, click the **Index** tab. To search for information using a keyword, click the **Search** tab.

To open context-sensitive help, click the window help icon (). A second browser window appears, which includes information for the window that you are currently viewing.

Links in Online Help

The online help contains links, indicated by blue underlined text. Clink a link to go to another help window or display a pop-up text box with additional information, such as a definition. Disable pop-up blocking in your browser to use this feature.

For more information about Trend Micro InterScan for Cisco CSC SSM, see the online help.

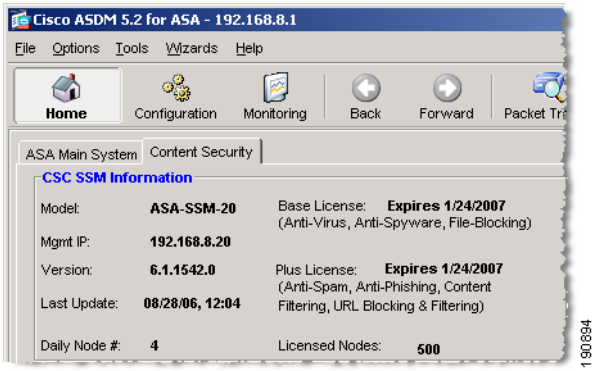
Licensing

As described in the introduction to this chapter, there are two levels of the Trend Micro InterScan for CSC SSM license: the Base License and the Plus License. The Base License provides antivirus, anti-spyware, and file blocking capability. The Plus License adds anti-spam, anti-phishing, content filtering, URL blocking, and URL filtering capability. The Base License is required for Plus license activation.

If you purchased only the Base License, you may be able to view unlicensed features on the CSC SSM console, but unlicensed features are not operational. You can, however, view online help for an unlicensed feature. You can also purchase the additional functionality offered with the Plus License at a later time.

If you are not sure of which level of license your organization purchased, review the CSC SSM Information section of the Content Security tab, which summarizes your licensing information, as shown in Figure 1-9.

Figure 1-9 Location of Licensing Information on the Content Security Tab



Alternatively, on the CSC SSM console, choose **Administration > Product License** to display the Product License window. Scroll to the Plus License section of the window, and check the Status field. If this field is set to "Activated," you have the Plus License functionality. Otherwise, this field is set to "Not Activated."

Windows That Require Plus Licensing

Table 1-2 indicates which windows on the CSC SSM console are available with the Base License, and which are available only when you purchase the additional Plus License.

Table 1-2 Windows Available Based on License Type

Window Title	Base License	Plus License
Summary > Status/Mail (SMTP)/Mail (POP3)/Web (HTTP)/File Transfer (FTP)	x	
Mail (SMTP) > Scanning > Incoming > Target/Action/Notification	x	
Mail (SMTP) > Scanning > Outgoing > Target/Action/Notification	x	
Mail (SMTP) > Anti-spam > SMTP Incoming Anti-spam Target/Action		x
Mail (SMTP) > Content Filtering > Incoming > SMTP Incoming Content Filtering Target/Action/Notification		x
Mail (SMTP) > Content Filtering > Outgoing > SMTP Incoming Content Filtering Target/Action/Notification		x
Mail (SMTP) > Configuration > Message Filter/Disclaimer/Incoming Mail Domain	x	
Mail (POP3) > Scanning > POP3 Scanning > Target/Action/Notification	x	
Mail (POP3) > Anti-spam > POP3 Anti-spam Target/Action		x
Mail (POP3) > Content Filtering > POP3 Content Filtering Target/Action/Notification		x
Web (HTTP) > Scanning > Target/Webmail Scanning/Action/Notification	x	
Web (HTTP) > File Blocking > Target/Notification	x	

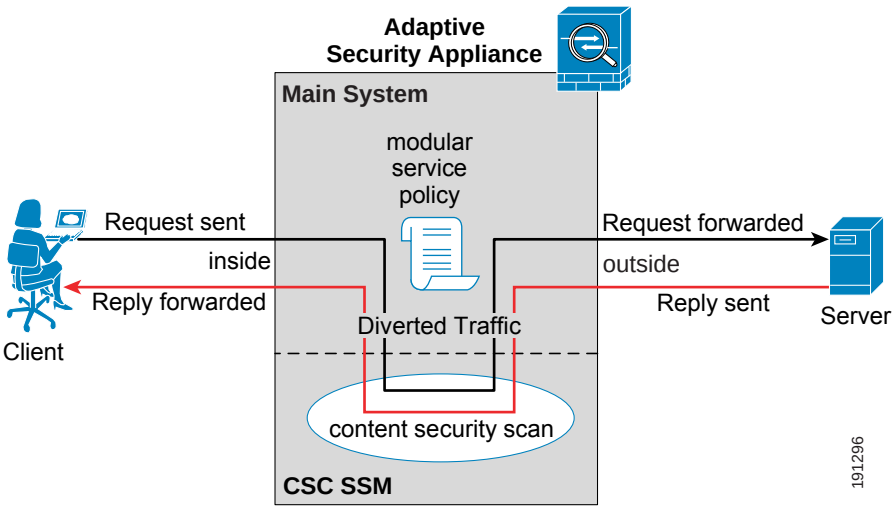
Table 1-2 Windows Available Based on License Type (continued)

Window Title	Base License	Plus License
Web (HTTP) > URL Blocking > Via Local List/PhishTrap/Notification		x
Web (HTTP) > URL Filtering > Filtering Rules		x
Web (HTTP) > URL Filtering > Settings > URL Filtering Settings URL Categories/Exceptions/Schedule/Re-classify URL		x
File Transfer (FTP) > Scanning > FTP Scanning Target/Action/Notification	x	
File Transfer (FTP) > File Blocking> Action/Notification	x	
Update > all windows	x	
Logs > all windows	x	
Administration > all windows	x	

Process Flow

Figure 1-10 illustrates the flow of traffic when the CSC SSM is installed in the adaptive security appliance. A request is sent from a client workstation to a server. As the request is processed through the adaptive security appliance, it is diverted to CSC SSM for content security scanning. If no security risk is detected, the request is forwarded to the server. The reply follows the same pattern, but in the reverse direction.

Figure 1-10 Process Flow



If a security risk is detected, it can be cleaned or removed, depending on how you have configured the CSC SSM.