



About This Guide	xi
Document Objectives	xi
Audience	xi
Document Organization	xii
Document Conventions	xii
Related Documentation	xiii
Obtaining Documentation	xiii
Cisco.com	xiii
Product Documentation DVD	xiii
Ordering Documentation	xiv
Documentation Feedback	xiv
Cisco Product Security Overview	xiv
Reporting Security Problems in Cisco Products	xv
Product Alerts and Field Notices	xv
Obtaining Technical Assistance	xvi
Cisco Technical Support & Documentation Website	xvi
Submitting a Service Request	xvii
Definitions of Service Request Severity	xvii
Obtaining Additional Publications and Information	xvii

CHAPTER 1

Introducing the CSC SSM	1-1
Overview	1-1
Features and Benefits	1-2
Available Documentation	1-3
Terminology	1-4
Introducing the Content Security Tab	1-4
Configuring Content Security	1-4
Introducing the CSC SSM Console	1-6
Navigation Pane	1-7
Tab Behavior	1-7
Save Button	1-8
Default Values	1-8
Tooltips	1-8

Online Help	1-9
Links in Online Help	1-10
Licensing	1-10
Windows That Require Plus Licensing	1-11
Process Flow	1-12

CHAPTER 2

Verifying Initial Setup	2-1
Verifying ASA Clock Setup	2-1
Verifying CSC SSM Activation	2-1
Verifying Scanning	2-2
Testing the Antivirus Feature	2-3
Verifying Component Status	2-4
Viewing the Status LED	2-5
Understanding SSM Management Port Traffic	2-6

CHAPTER 3

Configuring SMTP and POP3 Mail Traffic	3-1
Default Mail Scanning Settings	3-1
Defining Incoming and Outgoing SMTP Mail	3-2
Enabling SMTP and POP3 Spyware and Grayware Detection	3-3
Reviewing SMTP and POP3 Notifications	3-3
Types of Notifications	3-4
Modifying Notifications	3-4
Configuring SMTP Settings	3-5
Enabling SMTP and POP3 Spam Filtering	3-6
Enabling SMTP and POP3 Content Filtering	3-7
Enabling Network Reputation Services	3-8
About RBL+ and QIL	3-9

CHAPTER 4

Configuring Web (HTTP) and File Transfer (FTP) Traffic	4-1
Default Web and FTP Scanning Settings	4-1
Downloading Large Files	4-2
Deferred Scanning	4-3
Detecting Spyware and Grayware	4-3
Scanning Webmail	4-4
File Blocking	4-4
URL Blocking	4-5
Blocking from the Via Local List Tab	4-6

Blocking from the Via Pattern File (PhishTrap) Tab 4-7

URL Filtering 4-8

Filtering Settings 4-8

Filtering Rules 4-9

CHAPTER 5

Managing Updates and Log Queries 5-1

Updating Components 5-1

Manual Update 5-2

Scheduled Update 5-2

Configuring Proxy Settings 5-3

Configuring System Log Message Settings 5-3

Viewing Log Data 5-4

Logging of Scanning Parameter Exceptions 5-5

CHAPTER 6

Administering Trend Micro InterScan for Cisco CSC SSM 6-1

Configuring Connection Settings 6-1

Managing Administrator E-mail and Notification Settings 6-2

Backing Up Configuration Settings 6-3

Exporting a Configuration 6-4

Importing a Configuration 6-4

Configuring Failover Settings 6-4

Installing Product Upgrades 6-6

Viewing the Product License 6-6

License Expiration 6-7

Licensing Information Links 6-8

Activating the Product 6-8

Renewing a License 6-9

CHAPTER 7

Monitoring Content Security 7-1

Features of the Content Security Tab 7-1

Monitoring Content Security 7-3

Monitoring Threats 7-3

Monitoring Live Security Events 7-5

Monitoring Software Updates 7-6

Monitoring Resources 7-7

CHAPTER 8**Troubleshooting Trend Micro InterScan
for Cisco CSC SSM 8-1**

Troubleshooting Installation	8-1
What To Do If Installation Fails	8-3
Troubleshooting Activation	8-4
Troubleshooting Basic Functions	8-4
Cannot Log On	8-4
Recovering a Lost Password	8-4
Summary Status and Log Entries Out of Synch	8-5
Delays in HTTP Connections	8-6
Access to Some Websites Is Slow or Inaccessible	8-6
Performing a Packet Capture	8-6
FTP Download Does Not Work	8-7
Reimaging or Recovery of CSC Module	8-7
Troubleshooting Scanning Functions	8-7
Cannot Update the Pattern File	8-8
Spam Not Being Detected	8-8
Cannot Create a Spam Stamp Identifier	8-8
Unacceptable Number of Spam False Positives	8-9
Cannot Accept Any Spam False Positives	8-9
Unacceptable Amount of Spam	8-9
Virus Is Detected but Cannot Be Cleaned	8-9
Virus Scanning Not Working	8-9
Scanning Not Working Because of Incorrect ASA Firewall Policy Configuration	8-10
Scanning Not Working Because the CSC SSM Is in a Failed State	8-10
Downloading Large Files	8-11
Restart Scanning Service	8-12
Troubleshooting Performance	8-13
CSC SSM Console Timed Out	8-13
Status LED Flashing for Over a Minute	8-13
SSM Cannot Communicate with ASDM	8-13
Logging in Without Going Through ASDM	8-13
CSC SSM Throughput is Significantly Less Than ASA	8-14
Using Knowledge Base	8-14
Using the Security Information Center	8-15
Understanding the CSC SSM System Log Messages	8-16
SSM Application Mismatch [1-105048]	8-18
Data Channel Communication Failure [3-323006]	8-18
Traffic Dropped Because of CSC Card Failure [3-421001]	8-18

Drop ASDP Packet with Invalid Encapsulation [3-421003]	8-19
Daily Node Count [5-421006]	8-19
Data Channel Communication OK [5-505010]	8-19
New Application Detected [5-505011]	8-19
Application Stopped [5-505012]	8-20
Application Version Changes [5-505013]	8-20
Skip Non-applicable Traffic [6-421002]	8-21
Account Host Toward License Limit [6-421005]	8-21
Traffic Dropped Because of CSC Card Failure [6-421007]	8-21
Failed to Inject Packet [7-421004]	8-22
Connection capacity has been reached	8-22
Connection capacity has been restored	8-22
CSC has actively disconnected a connection	8-23
CSC SSM status message	8-23
Failover service communication failed	8-24
Failover service email could not be sent	8-24
Failover service encountered an internal error	8-24
HTTP URL blocking event	8-25
HTTP URL filtering event	8-26
License upgrade notice	8-26
Resource availability of the CSC SSM falls below the desired level	8-26
Resource availability of the CSC SSM has been restored	8-27
Scan service failed	8-27
Scan service recovered	8-28
Scheduled update report	8-28
Service module cannot create FIFO	8-28
Service module encountered a problem when communicating with the ASA chassis	8-29
Service module informational report	8-29
Service module internal communication error	8-30
Service module show module 1 details	8-30
SMTP/POP3 anti-spam event	8-31
Spyware/Grayware detection event	8-31
Syslog adaptor starting	8-32
System monitor started	8-32
Time synchronization with the ASA chassis failed	8-32
Virus detection event	8-32
Before Contacting Cisco TAC	8-33

APPENDIX A

Reimaging and Configuring the CSC SSM Using the CLI A-1

Installation Checklist	A-1
Preparing to Reimage the Cisco CSC SSM	A-2
Reimaging the CSC SSM	A-4
Confirming the Installation	A-7
Viewing or Modifying Network Settings	A-8
Viewing Date and Time Settings	A-9
Viewing Product Information	A-9
Viewing or Modifying Service Status	A-9
Using Password Management	A-10
Changing the Current Password	A-10
Modifying the Password-reset Policy	A-11
Restoring Factory Default Settings	A-12
Troubleshooting Tools	A-12
Enabling Root Account	A-13
Showing System Information	A-13
Collecting Logs	A-15
Enabling Packet Tracing	A-15
Modifying Upload Settings	A-16
Resetting the Management Port Access Control	A-16
Pinging an IP Address	A-17
Exiting the Setup Wizard	A-17
Resetting the Configuration via the CLI	A-17

APPENDIX B

Using CSC SSM with Trend Micro Control Manager B-1

About Control Manager	B-1
Control Manager Interface	B-2
Using the Management Console	B-2
Opening the Control Manager Console	B-3
Accessing the HTTPS Management Console	B-3
About the Product Directory	B-4
Downloading and Deploying New Components	B-4
Deploying New Components from the TMCM Product Directory	B-5
Viewing Managed Products Status Summaries	B-5
Configuring CSC SSM Products	B-6
Issuing Tasks to the CSC SSM	B-6
Querying and Viewing Managed Product Logs	B-7

GLOSSARY

INDEX

