



Cisco AsyncOS for Web User Guide

8.0.5

Published: March 17, 2014

Cisco Systems, Inc.

www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: N/A

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco AsyncOS for Web User Guide

© 2014 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Introduction to the Product and the Release	1-1
Introduction to the Web Security Appliance	1-1
What's New in This Release	1-1
New Features in Release 8.0.5	1-2
New Features in Release 8.0.0	1-2
Using the Appliance Web Interface	1-4
Web Interface Browser Requirements	1-4
Accessing the Appliance Web Interface	1-4
Committing Changes in the Web Interface	1-5
Clearing Changes in the Web Interface	1-5
The Cisco SensorBase Network	1-5
SensorBase Benefits and Privacy	1-5
Enabling Participation in The Cisco SensorBase Network	1-5

CHAPTER 2

Deploy a Content Security Virtual Appliance	2-1
Overview of Deploy a Content Security Virtual Appliance	2-1
Task Overview	2-1
Migrating a Virtual Appliance to an Alternate Physical Host	2-1

CHAPTER 3

Connect, Install, and Configure	3-1
Overview of Connect, Install, and Configure	3-1
Task Overview for Connecting, Installing, and Configuring	3-1
Connecting the Appliance	3-2
Gathering Setup Information	3-5
System Setup Wizard	3-6
System Setup Wizard Reference Information	3-7
Network / System Settings	3-7
Network / Network Context	3-8
Network / Network Interfaces and Wiring	3-9
Network / Routes for Management and Data Traffic	3-9
Network / Transparent Connection Settings	3-11
Network / Administrative Settings	3-11

- Security / Security Settings 3-13
- Upstream Proxies 3-13
 - Upstream Proxies Task Overview 3-14
 - Creating Proxy Groups for Upstream Proxies 3-14
- Network Interfaces 3-15
 - IP Address Versions 3-15
 - Enabling or Changing Network Interfaces 3-16
- Using the P2 Data Interface for Web Proxy Data 3-17
 - Configuring TCP/IP Traffic Routes 3-18
 - Modifying the Default Route 3-19
 - Adding a Route 3-19
 - Saving and Loading Routing Tables 3-20
 - Deleting a Route 3-20
 - Configuring Transparent Redirection 3-20
 - Specifying a Transparent Redirection Device 3-20
 - Configuring WCCP Services 3-21
 - Increasing Interface Capacity Using VLANs 3-24
 - Configuring and Managing VLANs 3-25
- Redirect Hostname and System Hostname 3-29
 - Changing the Redirect Hostname 3-30
 - Changing the System Hostname 3-30
 - Configuring SMTP Relay Host Settings 3-30
 - Configuring an SMTP Relay Host 3-31
- DNS Settings 3-31
 - Split DNS 3-31
 - Clearing the DNS Cache 3-32
 - Editing DNS Settings 3-32
- Troubleshooting Connect, Install, and Configure 3-33

CHAPTER 4

- Connect the Appliance to a Cloud Web Security Tower 4-1**
 - Overview of Connect the Appliance to a Cloud Web Security Tower 4-1
 - Cloud Connector versus Standard Mode 4-2
 - Documentation 4-4
 - Deployment 4-5
 - Configuring the Cloud Connector 4-5
 - Step 1. Access the Web Interface for the Web Security Appliance 4-5
 - Step 2. Accept the License Agreement and Begin Setup. 4-5
 - Step 3. Configure **System Settings**: 4-6

Step 4. Set the Appliance Mode	4-6
Step 5. Configure Cloud Connector Settings	4-6
Step 6. Configure Network Interfaces and Wiring	4-7
Step 7. Configure Routes for Management and Data Traffic	4-7
Step 8. Configure Transparent Connection Settings	4-7
Step 9. Configure Administrative Settings	4-8
Step 10. Review and Install	4-8
Directory Group Policies in the Cloud	4-8
Sending Directory Groups to the Cloud	4-8
Bypassing the Cloud Proxy Server	4-9
FTP and HTTPS	4-9
FTP	4-9
HTTPS	4-9
Preventing Loss of Secure Data	4-10
Cloud Connector Logs	4-10
Subscribing to the Cloud Connector Logs	4-10
Identities and User Authentication	4-11
Guest Access for Unauthenticated Users	4-11
Configuration Modes	4-11
Switching to Cloud Connector Mode	4-11

CHAPTER 5**Intercepting Web Requests 5-1**

Overview of Intercepting Web Requests	5-1
Tasks for Intercepting Web Requests	5-2
Best Practices for Intercepting Web Requests	5-2
Web Proxy Options for Intercepting Web Requests	5-3
Configuring Web Proxy Settings	5-3
Web Proxy Cache	5-5
Clearing the Web Proxy Cache	5-5
Removing URLs from the Web Proxy Cache	5-6
Specifying Domains or URLs that the Web Proxy never Cache	5-6
Choosing The Web Proxy Cache Mode	5-7
Web Proxy IP Spoofing	5-8
Web Proxy Custom Headers	5-9
Adding Custom Headers To Web Requests	5-9
Web Proxy Bypassing	5-10
Web Proxy Bypassing for Web Requests	5-10
Configuring Web Proxy Bypassing for Web Requests	5-10

- Configuring Web Proxy Bypassing for Applications 5-10
- Web Proxy Usage Agreement 5-11
- Client Options for Redirecting Web Requests 5-11
- Using PAC Files with Client Applications 5-11
 - Options For Publishing Proxy Auto-Config (PAC) Files 5-11
 - Client Options For Finding Proxy Auto-Config (PAC) Files 5-12
 - Automatic PAC File Detection 5-12
 - Hosting PAC Files on the Web Security Appliance 5-12
 - Specifying PAC Files in Client Applications 5-13
 - Configuring a PAC File Location Manually in Clients 5-13
 - Detecting the PAC File Automatically in Clients 5-13
- FTP Proxy Services 5-14
 - Overview of FTP Proxy Services 5-14
 - Enabling and Configuring the FTP Proxy 5-14
- SOCKS Proxy Services 5-16
 - Overview of SOCKS Proxy Services 5-16
 - Enabling Processing of SOCKS Traffic 5-16
 - Configuring the SOCKS Proxy 5-17
 - Creating SOCKS Policies 5-17
- Troubleshooting Intercepting Requests 5-18

CHAPTER 6

- Acquire End-User Credentials 6-1**
 - Overview of Acquire End-User Credentials 6-1
 - Authentication Task Overview 6-2
 - Authentication Best Practices 6-2
 - Credentials 6-2
 - Configuring Single-Sign-on 6-2
 - Tracking Credentials for Reuse During a Session 6-3
 - Authentication and Authorization Failures 6-3
 - Authentication Realms 6-3
 - About Authentication Realms 6-3
 - Creating an Active Directory Realm for Kerberos Authentication Scheme 6-3
 - Creating an Active Directory Authentication Realm 6-6
 - Creating an LDAP Authentication Realm 6-7
 - About Deleting Authentication Realms 6-11
 - Configuring Global Authentication Settings 6-12
 - Authentication Sequences 6-17
 - About Authentication Sequences 6-17

Creating Authentication Sequences	6-18
Editing And Reordering Authentication Sequences	6-18
Deleting Authentication Sequences	6-19
Failed Authentication	6-19
About Failed Authentication	6-19
Bypassing Authentication	6-20
Permitting Unauthenticated Traffic While Authentication Service is Unavailable	6-20
Granting Guest Access After Failed Authentication	6-20
Define an Identity that Supports Guest Access	6-21
Use an Identity that Supports Guest Access in a Policy	6-21
Configure How Guest User Details are Logged	6-21
Failed Authorization: Allowing Re-Authentication with Different Credentials	6-22
About Allowing Re-Authentication with Different Credentials	6-22
Allowing Re-Authentication with Different Credentials	6-22
Tracking Identified Users	6-22
Tracking Re-Authenticated Users	6-23
Credentials	6-24
Credential Format	6-24
Credential Encryption for Basic Authentication	6-24
About Credential Encryption for Basic Authentication	6-24
Configuring Credential Encryption	6-24
Troubleshooting Authentication	6-25

CHAPTER 7**Classify End-Users and Client Software** 7-1

Overview of Classify Users and Client Software	7-1
Classify Users and Client Software: Best Practices	7-2
Identity Criteria	7-2
Classifying Users and Client Software	7-3
Identities and Authentication	7-7
Troubleshooting Identities	7-8

CHAPTER 8**SaaS Access Control** 8-1

Overview of SaaS Access Control	8-1
Authenticate SaaS Users	8-2
Certificates and Keys	8-2
Configuring the Appliance as an Identity Provider	8-2
Using SaaS Access Control and Multiple Web Security Appliances	8-4
Creating SaaS Application Authentication Policies	8-4

Configuring End-User Access to the Single Sign-On URL 8-6

CHAPTER 9

Classify URLs for Policy Application 9-1

- Overview of Categorizing URL Transactions 9-1
 - Categorization of Failed URL Transactions 9-2
 - Enabling the Dynamic Content Analysis Engine 9-2
 - Uncategorized URLs 9-2
 - Matching URLs to URL Categories 9-3
 - Reporting Uncategorized and Misclassified URLs 9-3
 - URL Categories Database 9-3
- Configuring the URL Filtering Engine 9-4
- Managing Updates to the Set of URL Categories 9-4
 - Understanding the Impacts of URL Category Set Updates 9-5
 - Effects of URL Category Set Changes on Policy Group Membership 9-5
 - Effects of URL Category Set Updates on Filtering Actions in Policies 9-5
 - Merged Categories - Examples 9-6
 - Controlling Updates to the URL Category Set 9-7
 - Manually Updating the URL Category Set 9-7
 - Default Settings for New and Changed Categories 9-8
 - Verifying Existing Settings and/or Making Changes 9-8
 - Receiving Alerts About Category and Policy Changes 9-8
 - Responding to Alerts about URL Category Set Updates 9-8
- Filtering Transactions Using URL Categories 9-9
 - Configuring URL Filters for Access Policy Groups 9-9
 - Configuring URL Filters for Decryption Policy Groups 9-11
 - Configuring URL Filters for Data Security Policy Groups 9-12
- Creating and Editing Custom URL Categories 9-13
- Filtering Adult Content 9-15
 - Enforcing Safe Searches and Site Content Ratings 9-15
 - Logging Adult Content Access 9-16
- Redirecting Traffic in the Access Policies 9-17
 - Logging and Reporting 9-17
- Warning Users and Allowing Them to Continue 9-17
 - Configuring Settings for the End-User Filtering Warning Page 9-18
- Creating Time Based URL Filters 9-19
- Viewing URL Filtering Activity 9-19
 - Understanding Unfiltered and Uncategorized Data 9-19
 - Access Log File 9-20

Regular Expressions	9-20
Forming Regular Expressions	9-20
Regular Expression Character Table	9-22
URL Category Descriptions	9-22

CHAPTER 10

Create Policies to Control Internet Requests	10-1
Overview of Policies: Control Intercepted Internet Requests	10-1
Managing Web Requests Through Policies Task Overview	10-2
Managing Web Requests Through Policies Best Practices	10-2
Policies	10-2
Policy Types	10-3
Policy Order	10-5
Creating a Policy	10-5
Policy Configuration	10-10
Block, Allow, or Redirect Transaction Requests	10-11
Client Applications	10-11
About Client Applications	10-11
Using Client Applications in Policies	10-12
Exempting Client Applications from Authentication	10-13
Limiting Access by Time of Day	10-13
About Limiting Access by Time of Day	10-13
Creating a Time Range	10-13
Using Limiting Access by Time of Day in Policies	10-14
Controlling Access by URL Category	10-14
About Controlling Access by URL Category	10-14
Creating Custom URL Categories	10-15
Using URL Categories to Identify Web Requests	10-16
Using URL Categories to Action Web Request	10-16
Remote Users	10-17
About Remote Users	10-17
Configuring Identification for Remote Users	10-18
Configuring Identification of Remote Users	10-18
Display Remote User Status and Statistics for ASAs	10-19
Troubleshooting Policies	10-19

CHAPTER 11

Create Decryption Policies to Control HTTPS Traffic	11-1
Overview of Create Decryption Policies to Control HTTP Traffic	11-1
Managing HTTPS Traffic through Decryption Policies Task Overview	11-2

- Managing HTTPS Traffic through Decryption Policies Best Practices 11-2
- Decryption Policies 11-2
 - Enabling the HTTPS Proxy 11-3
 - Controlling HTTPS Traffic 11-4
 - Configuring Decryption Options 11-4
 - Authentication and HTTPS Connections 11-5
- Certificates 11-5
 - Managing Certificate Validation and Decryption for HTTPS 11-6
 - Valid Certificates 11-6
 - Invalid Certificate Handling 11-7
 - Uploading a Root Certificate and Key 11-7
 - Generating a Certificate and Key 11-8
 - Configuring Invalid Certificate Handling 11-8
 - Options for Certificate Revocation Status Checking 11-9
 - Enabling Real-Time Revocation Status Checking 11-10
 - Trusted Root Certificates 11-10
 - Adding Certificates to the Trusted List 11-11
 - Removing Certificates from the Trusted List 11-11
- Routing HTTPS Traffic 11-11
- Troubleshooting Decryption/HTTPS/Certificates 11-12

CHAPTER 12

- Scan Outbound Traffic for Existing Infections 12-1**
 - Overview of Scanning Outbound Traffic 12-1
 - User Experience with Blocked Requests 12-1
 - Understanding Upload Requests 12-2
 - Criteria for Group Membership 12-2
 - Matching Client Requests to Outbound Malware Scanning Policy Groups 12-2
 - Creating Outbound Malware Scanning Policies 12-3
 - Controlling Upload Requests 12-4
 - Logging 12-6

CHAPTER 13

- Configuring Security Services 13-1**
 - Overview of Configuring Security Services 13-1
 - Overview of Web Reputation Filters 13-2
 - Web Reputation Scores 13-2
 - Understanding How Web Reputation Filtering Works 13-3
 - Web Reputation in Access Policies 13-3
 - Web Reputation in Decryption Policies 13-4

Web Reputation in Cisco IronPort Data Security Policies	13-4
Overview of Anti-Malware Scanning	13-4
Understanding How the DVS Engine Works	13-5
Working with Multiple Malware Verdicts	13-5
Webroot Scanning	13-6
McAfee Scanning	13-6
Matching Virus Signature Patterns	13-6
Heuristic Analysis	13-6
McAfee Categories	13-7
Sophos Scanning	13-7
Understanding Adaptive Scanning	13-7
Adaptive Scanning and Access Policies	13-7
Enabling Anti-Malware and Reputation Filters	13-8
Configuring Anti-Malware and Reputation in Policies	13-9
Anti-Malware and Reputation Settings in Access Policies	13-10
Configuring Anti-Malware and Reputation Settings with Adaptive Scanning Enabled	13-10
Configuring Anti-Malware and Reputation Settings with Adaptive Scanning Disabled	13-11
Configuring Web Reputation Scores	13-12
Configuring Web Reputation Score Thresholds for Access Policies	13-12
Configuring Web Reputation Filter Settings for Decryption Policy Groups	13-13
Configuring Web Reputation Filter Settings for Data Security Policy Groups	13-13
Maintaining the Database Tables	13-14
The Web Reputation Database	13-14
Logging	13-14
Logging Adaptive Scanning	13-14
Caching	13-14
Malware Category Descriptions	13-15

CHAPTER 14**File Reputation Filtering and File Analysis 14-1**

Overview of File Reputation Filtering and File Analysis	14-1
File Threat Verdict Updates	14-1
File Processing Overview	14-2
Which Files Can Be Evaluated and Analyzed?	14-3
FIPS Compliance	14-3
Configuring File Reputation and Analysis Features	14-3
Requirements for Communication with File Reputation and Analysis Services	14-3
Routing Traffic to File Reputation and File Analysis Servers Through a Data Interface	14-4
Enabling File Reputation and Analysis Services	14-4

- Enabling File Reputation and Analysis Services Per Access Policy 14-5
- Ensuring That You Receive Alerts 14-5
- File Reputation and File Analysis Reporting and Tracking 14-6
 - Identifying Files by SHA-256 Hash 14-6
 - File Reputation and File Analysis Report Pages 14-6
 - Viewing File Reputation Filtering Data in Other Reports 14-7
 - About Web Tracking and Advanced Malware Protection Features 14-7
- Taking Action When File Threat Verdicts Change 14-8
- Troubleshooting File Reputation and Analysis 14-8
 - Log Files 14-8
 - Multiple Alerts About Failed File Reputation Queries 14-9
 - Alert About Failed File Upload for Analysis 14-9

CHAPTER 15

Managing Access to Web Applications 15-1

- Overview of Managing Access to Web Applications 15-1
- Understanding Application Control Settings 15-2
 - AVC Engine Updates 15-3
 - User Experience with Blocked Requests 15-3
- Enabling the AVC Engine 15-3
 - Configuring Application Control Settings in an Access Policy Group 15-4
- Controlling Bandwidth 15-4
 - Configuring Overall Bandwidth Limits 15-5
 - Configuring User Bandwidth Limits 15-5
 - Configuring the Default Bandwidth Limit for an Application Type 15-5
 - Overriding the Default Bandwidth Limit for an Application Type 15-6
 - Configuring Bandwidth Controls for an Application 15-6
- Controlling Instant Messaging Traffic 15-6
- Viewing AVC Activity 15-7
 - Access Log File 15-7

CHAPTER 16

Prevent Loss of Sensitive Data 16-1

- Overview of Prevent Loss of Sensitive Data 16-1
 - Bypassing Upload Requests Below a Minimum Size 16-2
 - User Experience with Blocked Requests 16-2
- Managing Upload Requests 16-2
- Managing Upload Requests on an External DLP System 16-3
- Evaluating Data Security and External DLP Policy Group Membership 16-4
 - Matching Client Requests to Data Security and External DLP Policy Groups 16-4

Creating Data Security and External DLP Policies	16-5
Managing Settings for Upload Requests	16-7
URL Categories	16-8
Web Reputation	16-8
Content Blocking	16-8
Defining External DLP Systems	16-9
Configuring External DLP Servers	16-9
Controlling Upload Requests Using External DLP Policies	16-11
Logging	16-11

CHAPTER 17

Notify End-Users of Proxy Actions	17-1
End-User Notifications Overview	17-1
Notification Best Practices	17-2
Editing On-Box End-User Notification Pages	17-2
Entering the custom URL for notification pages:	17-3
Enabling the End-user Acknowledgment Page	17-3
General Notification Settings	17-3
About General Settings for Notification Pages	17-4
Configuring General Settings for Notification Pages	17-4
On-Box End-User Notification Pages	17-4
Configuring On-Box End-User Notification Pages	17-4
Editing On-Box End-User Notification Pages	17-5
Use Variables in Customized On-Box End-User Notification Pages	17-7
Off-Box End-User Notification Pages	17-8
End-User Notification Page Parameters	17-8
Redirecting End-User Notification Pages to a Custom URL	17-9
End-User Acknowledgment Page	17-10
Configuring the End-User Acknowledgment Page	17-11
Access HTTPS and FTP Sites with the End-User Acknowledgment Page	17-12
Configuring the End-User URL Filtering Warning Page	17-12
Configuring FTP Notification Messages	17-13
Custom Text in Notification Pages	17-13
Supported HTML Tags in Notification Pages	17-13
Custom Text and Logos: Authentication, and End-User Acknowledgment Pages	17-14
Notification Page Types	17-15

CHAPTER 18

Generate Reports to Monitor End-user Activity	18-1
Overview of Reporting	18-1

- Working with Usernames in Reports 18-1
- Report Pages 18-2
- Using the Reporting Tab 18-2
 - Changing the Time Range 18-2
 - Searching Data 18-3
 - Choosing Which Data to Chart 18-4
- Custom Reports 18-4
 - Creating Your Custom Report Page 18-5
- Working with Columns on Report Pages 18-5
 - Configuring Columns on Report Pages 18-6
 - Subdomains vs. Second-Level Domains in Reporting and Tracking 18-7
 - Printing and Exporting Reports from Report Pages 18-7
 - Exporting Report Data 18-7
- Enabling Centralized Reporting 18-8
- Scheduling Reports 18-8
 - Adding a Scheduled Report 18-9
 - Editing Scheduled Reports 18-9
 - Deleting Scheduled Reports 18-10
- Generating Reports On Demand 18-10
- Archived Reports 18-10
- SNMP Monitoring 18-11
 - MIB Files 18-11
 - Hardware Objects 18-12
 - Hardware Traps 18-12
 - SNMP Traps 18-12
 - CLI Example 18-13

CHAPTER 19

- Web Security Appliance Reports 19-1**
 - Overview Page 19-1
 - Users Page 19-2
 - User Details Page 19-3
 - Web Sites Page 19-3
 - URL Categories Page 19-3
 - URL Category Set Updates and Reports 19-4
 - Application Visibility Page 19-4
 - Anti-Malware Page 19-5
 - Malware Category Report Page 19-5
 - Malware Threat Report Page 19-5

Advanced Malware Protection Page	19-5
File Analysis Page	19-6
AMP Verdict Updates Page	19-6
Client Malware Risk Page	19-6
Client Detail Page for Web Proxy - Clients by Malware Risk	19-6
Web Reputation Filters Page	19-7
L4 Traffic Monitor Page	19-7
SOCKS Proxy Page	19-8
Reports by User Location Page	19-8
Web Tracking Page	19-8
Searching for Transactions Processed by the Web Proxy	19-9
Searching for Transactions Processed by the L4 Traffic Monitor	19-11
Searching for Transactions Processed by the SOCKS Proxy	19-11
System Capacity Page	19-11
System Status Page	19-12

CHAPTER 20**Detecting Rogue Traffic on Non-Standard Ports** 20-1

Overview of Detecting Rogue Traffic	20-1
Configuring the L4 Traffic Monitor	20-1
List of Known Sites	20-2
Configuring L4 Traffic Monitor Global Settings	20-2
Updating L4 Traffic Monitor Anti-Malware Rules	20-3
Creating a Policy to Detect Rogue Traffic	20-3
Valid Formats	20-4
Viewing L4 Traffic Monitor Activity	20-4
Monitoring Activity and Viewing Summary Statistics	20-5
L4 Traffic Monitor Log File Entries	20-5

CHAPTER 21**Monitor System Activity Through Logs** 21-1

Overview of Logging	21-1
Tasks for Logging	21-2
Best Practices for Logging	21-2
Planning For Logging	21-2
Log Types	21-2
Log Subscriptions	21-3
Default Log Subscriptions	21-3
Log File Names and Appliance Directory Structure	21-3

- Archiving Log Files Using Rollover 21-4
- Saving Disk Space By Compressing Log Files 21-4
- Reading and Interpreting Log Files 21-4
- Adding and Editing Log Subscriptions 21-5
 - Deleting a Log Subscription 21-8
 - Manually Rolling Over Log Subscriptions 21-9
- Viewing Log Files 21-9
 - Viewing Log Files Using the Web Interface 21-9
 - Viewing Log Files Using the Command Line Interface 21-9
- Adding SCP SSH Public Host Keys to the Appliance 21-10
- Troubleshooting Web Proxy Issues Using Logs 21-11
- Access Log Files 21-12
 - Interpreting Access Log File Entries 21-12
 - Interpreting Access Log Scanning Verdict Entries 21-13
- W3C Compliant Access Log Files 21-15
 - W3C Field Types 21-15
 - Interpreting W3C Access Logs 21-15
 - W3C Log File Headers 21-15
 - W3C Field Prefixes 21-16
- Customizing Access Logs 21-17
 - Access Log User Defined Fields 21-17
 - Customizing Regular Access Logs 21-17
 - Customizing W3C Access Logs 21-18
- Traffic Monitor Log Files 21-18
 - Interpreting Traffic Monitor Logs 21-19
- Log File Types 21-19
- Log File Fields and Tags 21-23
 - Access and W3C Log File Fields 21-23
 - Transaction Result Codes 21-33
 - ACL Decision Tags 21-33
 - Malware Scanning Verdict Values 21-37
- Troubleshooting Logging 21-38

CHAPTER 22

Perform System Administration Tasks 22-1

- Overview of System Administration 22-1
- Saving and Loading the Appliance Configuration 22-2
 - Viewing and Printing the Appliance Configuration 22-2
 - Saving the Appliance Configuration File 22-2

Loading the Appliance Configuration File	22-2
Support Commands	22-3
Opening a Technical Support Request	22-3
Enabling Remote Access to the Web Security appliance	22-4
Packet Capture	22-4
Starting a Packet Capture	22-4
Managing Packet Capture Files	22-5
Working with Feature Keys	22-6
Displaying and Updating Feature Keys	22-6
Changing Feature Key Update Settings	22-6
Virtual Appliance License	22-7
Installing a Virtual Appliance License	22-7
Administering User Accounts	22-7
Managing Local User Accounts	22-8
Adding Local User Accounts	22-8
Deleting User Accounts	22-9
Editing User Accounts	22-9
Changing Passwords	22-9
RADIUS User Authentication	22-10
Sequence of Events For Radius Authentication	22-10
Enabling External Authentication Using RADIUS	22-10
Defining User Preferences	22-11
Configuring Administrator Settings	22-12
Configuring the Return Address for Generated Messages	22-13
Managing Alerts	22-13
Alert Classifications and Severities	22-13
Managing Alert Recipients	22-14
Adding and Editing Alert Recipients	22-14
Deleting Alert Recipients	22-14
Configuring Alert Settings	22-14
Alert Listing	22-15
Feature Key Alerts	22-16
Hardware Alerts	22-16
Logging Alerts	22-16
Reporting Alerts	22-17
System Alerts	22-19
Updater Alerts	22-20
Anti-Malware Alerts	22-20
FIPS Compliance	22-20

- FIPS Certificate Requirements **22-21**
- Enabling or Disabling FIPS Mode **22-21**
- System Date and Time Management **22-22**
 - Setting the Time Zone **22-22**
 - Synchronizing the System Clock with an NTP Server **22-22**
 - Deleting an NTP Server from the Configuration **22-22**
 - Manually Setting the System Date and Time in the GUI **22-23**
- Installing a Server Digital Certificate **22-23**
 - Obtaining Certificates **22-23**
 - Server Digital Certificate Requirements **22-23**
 - Certificate Signing Requests **22-24**
 - Intermediate Certificates **22-24**
 - Uploading Certificates to the Web Security Appliance **22-24**
- AsyncOS for Web Upgrades and Updates **22-26**
 - Best Practices For Upgrading AsyncOS for Web **22-26**
 - Upgrading and Updating AsyncOS and Security Service Components **22-27**
 - Upgrading AsyncOS for Web **22-27**
 - Automatic and Manual Update and Upgrade Queries **22-27**
 - Manually Updating Security Service Components **22-27**
 - Local And Remote Update Servers **22-28**
 - Updating and Upgrading from the Cisco Update Servers **22-28**
 - Upgrading from a Local Server **22-29**
 - Differences Between Local and Remote Upgrading Methods **22-30**
 - Configuring Upgrade and Service Update Settings **22-31**
- Reverting to a Previous Version of AsyncOS for Web **22-32**
 - Configuration File Use in the Revert Process **22-32**
 - Reverting AsyncOS for an Appliance Managed by the SMA **22-32**
 - Reverting AsyncOS for Web to a Previous Version **22-32**
- Authentication Problems **A-1**
 - LDAP Problems **A-2**
 - LDAP User Fails Authentication due to NTLMSSP **A-2**
 - LDAP Authentication Fails due to LDAP Referral **A-2**
 - Basic Authentication Problems **A-2**
 - Basic Authentication Fails **A-2**
 - Single Sign-On Problems **A-3**
 - Users Erroneously Prompted for Credentials **A-3**
- Browser Problems **A-3**
 - WPAD Not Working With Firefox **A-3**
- DNS Problems **A-3**

Alert: Failed to Bootstrap the DNS Cache	A-3
Feature Keys Expired	A-4
FTP Problems	A-4
URL Categories Do Not Block Some FTP Sites	A-4
Large FTP Transfers Disconnect	A-4
Zero Byte File Appears On FTP Servers After File Upload	A-4
HTTPS/Decryption/Certificate Problems	A-4
Accessing HTTPS Sites Using Routing Policies with URL Category Criteria	A-5
HTTPS Request Failures	A-5
HTTPS with IP-based Surrogates and Transparent Requests	A-5
Bypassing Decryption for Particular Websites	A-5
Alert: Problem with Security Certificate	A-6
Logging Problems	A-6
Custom URL Categories Not Appearing in Access Log Entries	A-6
Logging HTTPS Transactions	A-6
Alert: Unable to Maintain the Rate of Data Being Generated	A-7
Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs	A-7
Policy Problems	A-7
Access Policy not Configurable for HTTPS	A-7
Blocked Object Problems	A-8
Some Microsoft Office Files Not Blocked	A-8
Blocking DOS Executable Object Types Blocks Updates for Windows OneCare	A-8
Identity Disappeared from Policy	A-8
Policy Match Failures	A-8
Policy is Never Applied	A-8
HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication	A-9
User Matches Global Policy for HTTPS and FTP over HTTP Requests	A-9
User Assigned Incorrect Access Policy	A-9
Policy Troubleshooting Tool: Policy Trace	A-10
About the Policy Trace Tool	A-10
Tracing Client Requests	A-10
Customizing Request Details	A-11
Overriding Response Details	A-11
Problems with File Reputation and File Analysis	A-12
Site Access Problems	A-12
Cannot Access URLs that Do Not Support Authentication	A-12
Cannot Access Sites With POST Requests	A-13
Upstream Proxy Problems	A-13

Upstream Proxy Does Not Receive Basic Credentials	A-13
Client Requests Fail Upstream Proxy	A-13
Unable to Route FTP Requests Via an Upstream Proxy	A-13
WCCP Problems	A-14
Maximum Port Entries	A-14
Overview of the Command Line Interface	B-1
Accessing the Command Line Interface	B-1
Working with the Command Prompt	B-2
Command Syntax	B-2
Select Lists	B-2
Yes/No Queries	B-3
Subcommands	B-3
Escaping Subcommands	B-3
Command History	B-4
Completing Commands	B-4
Committing Configuration Changes	B-4
General Purpose CLI Commands	B-4
Committing Configuration Changes	B-4
Clearing Configuration Changes	B-5
Exiting the Command Line Interface Session	B-5
Seeking Help on the Command Line Interface	B-6
Web Security Appliance CLI Commands	B-6
Documentation Set	C-1
Training	C-1
Knowledge Base	C-2
Cisco Support Community	C-2
Customer Support	C-2
Third Party Contributors	C-2
Cisco Welcomes Your Comments	C-3
Cisco Systems End User License Agreement	D-1
Supplemental End User License Agreement for Cisco Systems Content Security Software	D-8



Introduction to the Product and the Release

- [Introduction to the Web Security Appliance, page 1-1](#)
- [What's New in This Release, page 1-1](#)
- [Using the Appliance Web Interface, page 1-3](#)
- [The Cisco SensorBase Network, page 1-4](#)

Introduction to the Web Security Appliance

The Cisco Web Security Appliance intercepts and monitors internet traffic and applies policies to help keep your internal network secure from malware, sensitive data loss, productivity loss, and other internet-based threats.

What's New in This Release



The following new features and enhancements have been added in this release.

- [New Features in Release 8.0.5](#)
- [New Features in Release 8.0.0](#)

New Features in Release 8.0.5

Feature	Description
Advanced Malware Protection provides file reputation and analysis services	<p>Advanced Malware Protection (AMP) is an additionally licensed feature available to all Cisco Web Security appliance customers. AMP is a comprehensive malware-defeating solution that enables malware detection and blocking, continuous analysis, and retrospective alerting. It takes advantage of the vast Cisco cloud security intelligence networks.</p> <p>AMP augments the anti-malware detection and blocking capabilities already offered by Cisco Web Security appliances with enhanced file reputation capabilities, detailed file behavior reporting, continuous file analysis, and retrospective verdict alerting.</p> <p>For details, see Chapter 14, “File Reputation Filtering and File Analysis.”</p>

New Features in Release 8.0.0

Feature	Description
New Features	
Cloud Web Security Connector	<p>The 8.0 release introduces a new configuration mode, which allows you to connect to and direct traffic to Cisco Cloud Web Security for policy enforcement and threat defense. Documentation for the Cloud Connector is in Chapter 3 of the User Guide, “Connect the Appliance to a Cloud Web Security Tower.” To put the Web Security appliance in Cloud Connector mode, begin with “Configuring the Cloud Connector.”</p> <hr/> <p> Note After upgrading to AsyncOS 8.0, if you plan to use the appliance in Cloud Connector mode, do not put the appliance into Standard mode using the System Setup Wizard. Put the appliance directly into Cloud Connector mode.</p>
Kerberos Authentication	<p>Kerberos is a "pass through" authentication protocol for Windows, Mac OS X, and other operating systems. Due to many operating systems today that no longer support NTLM or NTLM SSO, Kerberos has become a very popular authentication protocol. This feature supports Kerberos Version 5 (MS KRB5 and KRB5), and AD servers such as 2003, 2008, 2008R2, and 2012. We also support the following internet browsers: Internet Explorer, Chrome, Firefox and Safari.</p> <hr/> <p> Note Active Directory realms created with appliances using AsyncOS versions prior to 8.0 will not have the Kerberos scheme available.</p>

Feature	Description
Cisco Web Security Virtual Appliance	<p>Cisco offers the Cisco Web Security appliance as a virtual machine that you can host on your own network.</p> <p>The virtual appliance requires a separate license for the virtual appliance purchased from Cisco and a Cisco UCS Server (Blade or Rack-Mounted) hardware platform running VMware ESXi version 4.x, 5.0, or 5.1.</p> <p>The <i>Cisco Content Security Virtual Appliance Installation Guide</i> includes more information on the requirements for the virtual appliance.</p> <p>The new Web Security virtual appliance models and configurations are:</p> <ul style="list-style-type: none"> • S000V (250 GB disk space, 50 GB cache space, 1 core, 4 GB memory) • S100V (250 GB disk space, 50 GB cache space, 2 cores, 6 GB memory) • S300V (1024 GB disk space, 200 GB cache space, 4 cores, 8 GB memory) <p>This feature includes the following changes to AsyncOS for Web:</p> <ul style="list-style-type: none"> • The Web Security virtual appliance license allows you to clone and run multiple virtual appliances on your network. • The loadlicense CLI command for installing the virtual appliance license. • You can use the same license for multiple virtual appliances. <p>Feature keys are included as part of the virtual appliance license. The feature keys will expire at the same time as the license. Purchasing new feature keys will require downloading and installing a new virtual appliance license.</p> <p>Due to feature keys being included in the virtual appliance license, there are no 30-day evaluations for AsyncOS features.</p> <p>You cannot open a Technical Support tunnel before installing the virtual appliance license.</p> <p>The version, ipcheck, and support request CLI commands have also been updated to included virtual appliance information.</p> <p>There are new alerts and logs for misconfigured virtual appliances.</p> <p>See the <i>Cisco Content Security Virtual Appliance Installation Guide</i> at http://www.cisco.com/en/US/products/ps10164/prod_installation_guides_list.html.</p>
IPv6 Support	<p>IPv6 is supported in both explicit and transparent deployment modes. The IPv6 feature is designed to have the same familiar configuration interface as IPv4. Existing features such as HTTP/HTTPS/FTP, L4TM, Proxy bypass, URL categorization, AVC, among many others all are IPv6 ready. Logs and reports are largely unchanged but offer additional visibility into IPv6 traffic.</p>
Enhancements	
User Interface	<p>AsyncOS 8.0.0 introduces an easier to use interface that allows "drag and drop" capabilities. The "view reports" page, favorites page, and other interfaces allow user to drag and drop to rearrange items on the screen, such as ordering a list or moving components of the reports dashboard to a different location.</p>

Related Topics

- Product release notes:
http://www.cisco.com/en/US/partner/products/ps10164/prod_release_notes_list.html

Using the Appliance Web Interface

- [Web Interface Browser Requirements](#), page 1-3
- [Accessing the Appliance Web Interface](#), page 1-3
- [Committing Changes in the Web Interface](#), page 1-4
- [Clearing Changes in the Web Interface](#), page 1-4

Web Interface Browser Requirements

To access the web interface, your browser must support and be enabled to accept JavaScript and cookies. It must be able to render HTML pages containing Cascading Style Sheets (CSS).

The Cisco Web Security Appliance follows the Target Environments set by YUI:
<http://yuilibrary.com/yui/environments/>

Your session automatically times out after 30 minutes of inactivity.

Some buttons and links in the web interface cause additional windows to open. Therefore, you may need to configure the browser's pop-up blocking settings in order to use the web interface.

**Note**

Only use one browser window or tab at a time to edit the appliance configuration. Also, do not edit the appliance using the web interface and the CLI at the same time. Editing the appliance from multiple places concurrently results in unexpected behavior and is not supported.

Accessing the Appliance Web Interface

- Step 1** Open a browser and enter the IP address (or hostname) of the Web Security appliance. If the appliance has not been previously configured, use the default settings:

```
https://192.168.42.42:8443
```

-or-

```
http://192.168.42.42:8080
```

where 192.168.42.42 is the default IP address, and 8080 is the default admin port setting for HTTP, and 8443 is default admin port for HTTPS.

Otherwise, if the appliance is currently configured, use the IP address (or hostname) of the M1 port.

**Note**

You must use a port number when connecting to the appliance (by default, port 8080). Failing to specify a port number when accessing the web interface results in a default port 80, Proxy Unlicensed error page.

- Step 2** When the appliance login screen appears, enter the username and password to access the appliance. By default, the appliance ships with the following username and password:

- Username: **admin**
 - Password: **ironport**
-

Committing Changes in the Web Interface



Note You can make multiple configuration changes before you commit all of them.

- Step 1** Click the **Commit Changes** button.
 - Step 2** Enter comments in the Comment field if you choose.
 - Step 3** Click **Commit Changes**.
-

Clearing Changes in the Web Interface

- Step 1** Click the **Commit Changes** button.
 - Step 2** Click **Abandon Changes**.
-

The Cisco SensorBase Network

The Cisco SensorBase Network is a threat management database that tracks millions of domains around the world and maintains a global watch list for Internet traffic. SensorBase provides Cisco with an assessment of reliability for known Internet domains. The Web Security appliance uses the SensorBase data feeds to improve the accuracy of Web Reputation Scores.

SensorBase Benefits and Privacy

Participating in the Cisco SensorBase Network means that Cisco collects data and shares that information with the SensorBase threat management database. This data includes information about request attributes and how the appliance handles requests.

Cisco recognizes the importance of maintaining your privacy, and does not collect or use personal or confidential information such as usernames and passwords. Additionally, the file names and URL attributes that follow the hostname are obfuscated to ensure confidentiality. When it comes to decrypted HTTPS transactions, the SensorBase Network only receives the IP address, web reputation score, and URL category of the server name in the certificate.

If you agree to participate in the SensorBase Network, data sent from your appliance is transferred securely using HTTPS. Sharing data improves Cisco's ability to react to web-based threats and protect your corporate environment from malicious activity.

Enabling Participation in The Cisco SensorBase Network



Note Standard SensorBase Network Participation is enabled by default during system setup.

-
- Step 1** Choose to the **Security Services > SensorBase**.
- Step 2** Verify that SensorBase Network Participation is enabled.
When it is disabled, none of the data that the appliance collects is sent back to the SensorBase Network servers.
- Step 3** In the Participation Level section, choose one of the following levels:
- **Limited.** Basic participation summarizes server name information and sends MD5-hashed path segments to the SensorBase Network servers.
 - **Standard.** Enhanced participation sends the entire URL with unobfuscated path segments to the SensorBase Network servers. This option assists in providing a more robust database, and continually improves the integrity of Web Reputation Scores.
- Step 4** In the AnyConnect Network Participation field, choose whether or not to include information collected from clients that connect to the Web Security appliance using Cisco AnyConnect Client.
AnyConnect Clients send their web traffic to the appliance using the Secure Mobility feature.
- Step 5** In the Excluded Domains and IP Addresses field, optionally enter any domains or IP addresses to exclude from traffic sent to the SensorBase servers.
- Step 6** Submit and commit your changes.
-



Deploy a Content Security Virtual Appliance

- [Overview of Deploy a Content Security Virtual Appliance, page 2-1.](#)
- [Task Overview, page 2-1](#)
- [Migrating a Virtual Appliance to an Alternate Physical Host, page 2-1](#)

Overview of Deploy a Content Security Virtual Appliance

Cisco offers the Cisco Web Security appliance as a virtual machine that you can host on your own network. The virtual appliance requires a separate license for the virtual appliance purchased from Cisco and a Cisco UCS Server (Blade or Rack-Mounted) hardware platform running VMware ESXi version 4.x, 5.0, or 5.1.

Task Overview

Task	More Information
1. Connect, install, and configure the physical appliance.	Connect, Install, and Configure.
2. Use the loadlicense command to load the virtual appliance license.	<i>Cisco Content Security Virtual Appliance Installation Guide</i>
3. Use the provided worksheet to gather basic setup information.	Gathering Setup Information, page 3-5.
4. Run the System Setup Wizard on the virtual appliance.	System Setup Wizard, page 3-6.

Migrating a Virtual Appliance to an Alternate Physical Host

You can use VMware® VMotion™ to migrate a running virtual appliance to an alternate physical host:

Before You Begin

- Verify that both the physical hosts have the same network configuration.
- Verify that both physical hosts have access to the datastore (storage area network (SAN) or Network-attached storage (NAS)) for the appliance on which the appliance is based.

Migrating a Virtual Appliance to an Alternate Physical Host

- Verify that both physical hosts have access to the defined network(s) to which the appliance's interfaces are mapped.

Step 1 Migrate the virtual appliance using VMotion documentation.



Connect, Install, and Configure

- [Overview of Connect, Install, and Configure, page 3-1.](#)
- [Connecting the Appliance, page 3-2.](#)
- [Gathering Setup Information, page 3-5.](#)
- [System Setup Wizard, page 3-6](#)
- [Upstream Proxies, page 3-13](#)
- [Enabling or Changing Network Interfaces, page 3-16](#)
- [Using the P2 Data Interface for Web Proxy Data, page 3-17](#)
- [Changing the System Hostname, page 3-30](#)
- [DNS Settings, page 3-31](#)

Overview of Connect, Install, and Configure

The appliance works in conjunction with other network devices to intercept traffic. These can include switches, transparent redirection devices, network taps, and other proxy servers or Web Security appliances.

The appliance comes with multiple network ports, with each assigned to manage one or more specific data types.

The appliance uses network routes, DNS, VLANs, and other settings and services to manage network connectivity and traffic interception. The System Setup Wizard allows you to set up basic services and settings, and through the appliance web interface which allows you to modify settings or to configure additional options.

Task Overview for Connecting, Installing, and Configuring

Task	More Information
1. Connect the appliance to internet traffic.	Connecting the Appliance, page 3-2
2. Gather and record setup information.	Gathering Setup Information, page 3-5

Task	More Information
3. Run the System Setup Wizard.	System Setup Wizard, page 3-6
4. (Optional) Connect upstream proxies.	Upstream Proxies, page 3-13

Connecting the Appliance


Before You Begin

- Follow the instructions in the Cisco 170 Series Hardware Installation Guide to mount the appliance, cable the appliance for management, and connect the appliance to power.
- If you plan to physically connect the Appliance to a WCCP v2 router for transparent redirection, first verify that the WCCP router supports Layer 2 redirection.
- Be aware of Cisco configuration recommendations:
 - Use simplex cabling (separate cables for incoming and outgoing traffic) if possible for enhanced performance and security.

Step 1 Connect the Management interface if you have not already done so:

Ethernet Port	Notes
M1	<p>Connect M1 to where it can:</p> <ul style="list-style-type: none"> • Send and receive Management traffic. • (Optional) Send and receive web proxy data traffic. <p>You can connect a laptop directly to M1 to administer the appliance.</p> <p>To connect to the management interface using a hostname (<code>http://hostname:8080</code>), add the appliance hostname and IP address to your DNS server database.</p>
P1 and P2 (optional)	<ul style="list-style-type: none"> • Available for outbound management services traffic but not administration. • Enable "Restrict M1 port to appliance management services only" Network > Interfaces page. • Set routing for the service to use the Data interface.

Step 2 (Optional) Connect the appliance to data traffic either directly or through a transparent redirection device:

Ethernet Port	Explicit Forwarding	Transparent Redirection
P1/P2	<p>P1 only:</p> <ul style="list-style-type: none"> • Enable "Restrict M1 port to appliance management services only". • Connect P1 and M1 to different subnets. • Use a duplex cable to connect P1 the internal network and the internet to receive both inbound and outbound traffic. <p>P1 and P2</p> <ul style="list-style-type: none"> • Enable P1. • Connect M1, P1, and P2 to different subnets. • Connect P2 to the internet to receive inbound internet traffic. <p>After running the System Setup Wizard, enable P2.</p>	<p>Device: WCCP v2 router:</p> <ul style="list-style-type: none"> • For Layer 2 redirection, physically connect router to P1/P2. • For Layer 3 redirection, be aware of possible performance issues with Generic Routing Encapsulation. • Create a WCCP Service on the Appliance. <p>Device: Layer-4 Switch:</p> <ul style="list-style-type: none"> • For Layer 2 redirection, physically connect switch to P1/P2. • For Layer 3 redirection, be aware of possible performance issues with Generic Routing Encapsulation. <p> Note The appliance does not support inline mode.</p>
M1 (optional)	If "Restrict M1 port to appliance management services only" is disabled, M1 is the default port for data traffic.	N/A

- Step 3** (Optional) To monitor Layer-4 traffic, connect the Appliance to a TAP, switch, or hub after the proxy ports and before any device that performs network address translation (NAT) on client IP addresses:

Ethernet Port	Notes
T1/T2	<p>To allow Layer-4 Traffic Monitor blocking, put Layer 4Traffic Monitor on the same network as the Web Security appliance.</p> <p>Recommended configuration:</p> <p>Device: Network TAP:</p> <ul style="list-style-type: none"> • Connect T1 to network TAP to receive outbound client traffic. • Connect T2 to network TAP to receive inbound internet traffic. <p>Other options:</p> <p>Device: Network TAP:</p> <ul style="list-style-type: none"> • Use duplex cable on T1 to receive inbound and outbound traffic. <p>Device: Spanned or mirrored port on a switch</p> <ul style="list-style-type: none"> • Connect T1 to receive outbound client traffic and connect T2 to receive inbound internet traffic. • (Less preferred) Connect T1 using a half or full duplex cable to receive both inbound and outbound traffic. <p>Device: Hub:</p> <ul style="list-style-type: none"> • (Least preferred) Connect T1 using a duplex cable to receive both inbound and outbound traffic. <p>The appliance listens to traffic on all TCP ports on these interfaces.</p>

- Step 4** Connect external proxies upstream of the appliance to allow the external proxies to receive data from the appliance.

Next Step

- [Gathering Setup Information, page 3-5](#)

Related Topics

- [Enabling or Changing Network Interfaces, page 3-16](#)
- [Using the P2 Data Interface for Web Proxy Data, page 3-17](#)
- [Adding and Editing a WCCP Service, page 3-21](#)
- [Configuring Transparent Redirection, page 3-20](#)
- [Upstream Proxies, page 3-13](#)

Gathering Setup Information

You can use the worksheet below to record the configuration values you will need while running the System Setup Wizard. For additional information about each property, see [System Setup Wizard Reference Information, page 3-7](#).

System Setup Wizard Worksheet

Property	Value	Property	Value
Appliance Details		Routes	
Default System Hostname		Management Traffic	
Local DNS Server(s) (Required if not using Internet Root Servers)		Default Gateway	
DNS Server 1		(Optional) Static Route Table Name	
(Optional) DNS Server 2		(Optional) Static Route Table Destination Network	
(Optional) DNS Server 3		(Optional) Standard Service Router Addresses	
(Optional) Time Settings		(Optional) Data Traffic	
Network Time Protocol Server		Default Gateway	
(Optional) External Proxy Details		Static Route Table Name	
Proxy Group Name		Static Route Table Destination Network	
Proxy Server Address		(Optional) WCCP Settings	
Proxy Port Number		WCCP Router Address	
Interface Details		WCCP Router Password	
Management (M1) Port		Administrative Settings	
IPv4 Address (required)		Administrator Password	
IPv6 Address (optional)			
Network Mask		Email System Alerts To	
Hostname		(Optional) SMTP Relay Host	
(Optional) Data (P1) Port			
IPv4 (optional)			
IPv6 Address (optional)			
Network Mask			
Hostname			

System Setup Wizard

Before You Begin:

- Connect the Appliance to networks and devices. [Connecting the Appliance, page 3-2](#)
- Complete the System Setup Wizard worksheet. [Gathering Setup Information, page 3-5](#).
- If you are preparing to run the System Setup Wizard on a virtual appliance, use the `loadlicense` command to load the virtual appliance license. *Cisco Security Virtual Appliance Installation Guide*.
- Note that reference information for each configuration item used in the System Setup Wizard is available at [System Setup Wizard Reference Information, page 3-7](#).



Warning

Only use the System Setup Wizard the first time you install the appliance or if you want to completely overwrite the existing configuration.

Step 1 Open a browser and enter the IP address of the Web Security appliance. The first time you run the System Setup Wizard, use the default IP address:

```
https://192.168.42.42:8443
```

-or-

```
http://192.168.42.42:8080
```

where `192.168.42.42` is the default IP address, and `8080` is the default admin port setting for HTTP, and `8443` is default admin port for HTTPS.

Otherwise, if the appliance is currently configured, use the IP address of the M1 port.

Step 2 When the appliance login screen appears, enter the username and password to access the appliance. By default, the appliance ships with the following username and password:

- Username: **admin**
- Password: **ironport**

Step 3 Choose **System Administration > System Setup Wizard**.

Step 4 If the appliance is already configured, you will be warned that you are about to reset the configuration. To continue with the System Setup Wizard, click the **Reset Configuration** button. The appliance will reset and the browser will refresh to the appliance home screen. Begin again at [Step 3](#).

Step 5 Read and accept the terms of the end user license agreement.

Step 6 Click **Begin Setup** to continue.

Step 7 Configure all settings using the provided reference tables as required.

Step 8 Review the configuration information. If you need to change an option, click the **Edit** button for that section.

Step 9 Click **Install This Configuration**.

A *Next Steps* page should appear once the configuration installed. However, depending on the IP, hostname, or DNS settings you configured during setup, you may lose connection to the appliance at this stage. If a page not found is displayed in your browser, change the URL to reflect any new address settings and reload the page. Then continue with any post setup tasks you wish to perform.

System Setup Wizard Reference Information

Network / System Settings

Table 3-1

Property	Description
Default System Hostname	<p>The system hostname is the fully-qualified hostname used to identify the appliance in the following areas:</p> <ul style="list-style-type: none"> the command line interface (CLI) system alerts end-user notification and acknowledgement pages when forming the machine NetBIOS name when the Web Security appliance joins an Active Directory domain. <p>The system hostname does not correspond directly to interface hostnames and is not used by clients to connect to the appliance.</p>
DNS Server(s): Use the Internet's Root DNS Servers	<p>You can choose to use the Internet root DNS servers for domain name service lookups when the appliance does not have access to DNS servers on your network.</p> <p>Note Internet Root DNS servers will not resolve local hostnames. If you need the appliance to resolve local hostnames you must use a local DNS server or add the appropriate static entries to the local DNS using the Command Line Interface.</p>
DNS Server(s): Use these DNS Servers	<p>The local DNS server(s) that the appliance can use to resolve hostnames.</p>
NTP Server	<p>The Network Time Protocol (NTP) server used to synchronize the system clock with other servers on the network or the Internet.</p> <p>The default is time.sco.cisco.com.</p>
Time Zone	<p>Affects timestamps in message headers and log files.</p>

Related Topics

- [DNS Settings, page 3-31](#)

Network / Network Context



Note When you use the Web Security appliance in a network that contains another proxy server, it is recommended that you place the Web Security appliance downstream from the proxy server, closer to the clients.

Table 3-2

Property	Description
Is there another web proxy on your network?	<p>Is there another proxy on your network, such that</p> <ul style="list-style-type: none"> a. traffic must pass through it? b. it will be upstream of the Web Security appliance? <p>If yes for both points, select the checkbox. This allows you to create a proxy group for one upstream proxy. You can add more upstream proxies later.</p>
Proxy group name	A name used to identify the proxy group on the appliance.
Address	The hostname or IP address of the upstream proxy server.
Port	The port number of the upstream proxy server.

Related Topics

- [Upstream Proxies, page 3-13](#)

Network / Network Interfaces and Wiring

Table 3-3

Property	Description
Management	<p>The IP address, network mask, and hostname to use to manage the Web Security appliance and, by default, for proxy (data) traffic.</p> <p>Administrators can use the hostname specified here when connecting to the appliance management interface (or in browser proxy settings if M1 is used for proxy data), but you must register it in your organization's DNS.</p> <p>(Optional) Check the Use M1 Port For Management Only checkbox if you want to use a separate port for data traffic.</p> <p>Note When you use M1 for management traffic only, configure at least one data interface, on another subnet, for proxy traffic. You must also define different routes for management and data traffic.</p>
Data	<p>The IP address, network mask, and hostname to use for data traffic on the P1 port. This must use a different subnet to that used by the management port.</p> <p>Clients can use the hostname specified here (in browser proxy settings, for example) but you must register it in your organization's DNS.</p> <p>If you configure the M1 interface for management traffic only, you must configure the P1 interface for data traffic. However, you can configure the P1 interface even when the M1 interface is used for both management and data traffic.</p> <p>You can enable and configure the P1 port only in the System Setup Wizard. If you want to enable the P2 interface, you must do this after finishing the System Setup Wizard.</p>
Layer-4 Traffic Monitor	<p>The type of wired connections plugged into the "T" interfaces:</p> <ul style="list-style-type: none"> • Duplex TAP. The T1 port receives both incoming and outgoing traffic. • Simplex TAP. The T1 port receives outgoing traffic (from the clients to the Internet) and the T2 port receives incoming traffic (from the Internet to the clients). <p>Cisco recommends using Simplex when possible because it can increase performance and security.</p>

Network / Routes for Management and Data Traffic



Note If you enable "Use M1 port for management only", this section will have separate sections for

management and data traffic; otherwise one joint section will be shown.

Table 3-4

Property	Description
Default Gateway	The default gateway IP address to use for the traffic through the Management and Data interfaces.
Static Routes Table	Optional static routes for management and data traffic. Multiple routes can be added. A route gateway must reside on the same subnet as the Management or Data interface on which it is configured.

Network / Transparent Connection Settings

Table 3-5

Property	Description
Layer-4 Switch or No Device	Specifies that the Web Security appliance is connected to a layer 4 switch for transparent redirection, or that no transparent redirection device is used and clients will explicitly forward requests to the appliance.
WCCP v2 Router	<p>Specifies that the Web Security appliance is connected to a version 2 WCCP capable router.</p> <p>If you connect the appliance to a version 2 WCCP router, you must create at least one WCCP service. You can enable the standard service on this screen, or after the System Setup Wizard is finished, where you can also create multiple dynamic services.</p> <p>When you enable the standard service, you can also enable router security and enter a password. The password used here must be used all appliances and WCCP routers within the same service group.</p> <p>A standard service type (also known as the “web-cache” service) is assigned a fixed ID of zero, a fixed redirection method (by destination port), and a fixed destination port of 80.</p> <p>A dynamic service type allows you to define a custom ID, port numbers, and redirection and load balancing options.</p>

Network / Administrative Settings

Table 3-6

Property	Description
Administrator Password	The password used to access the Web Security appliance for administrative purposes.
Email System Alerts To	The email address to which the appliance sends systems alerts.
Send Email via SMTP Relay Host (optional)	<p>The address and port for an SMTP relay host that AsyncOS can use to send system generated email messages.</p> <p>If no SMTP relay host is defined, AsyncOS uses the mail servers listed in the MX record.</p>

Table 3-6

Property	Description
AutoSupport	Specifies whether or not the appliance sends system alerts and weekly status report to Cisco Customer Support.
SensorBase Network Participation	<p>Specifies whether or not to participate in the Cisco SensorBase Network. If you participate, you can configure Limited or Standard (full) participation. Default is Standard.</p> <p>The SensorBase Network is a threat management database that tracks millions of domains around the world and maintains a global watch list for Internet traffic. When you enable SensorBase Network Participation, the Web Security appliance sends anonymous statistics about HTTP requests to Cisco to increase the value of SensorBase Network data.</p>

Security / Security Settings

Table 3-7

Option	Description
Global Policy Default Action	Specifies whether to block or monitor all web traffic by default after the System Setup Wizard completes. You can change this behavior later by editing the Protocols and User Agents settings for the Global Access Policy. The default setting is to monitor traffic.
L4 Traffic Monitor	Specifies whether the Layer-4 Traffic Monitor should monitor or block suspected malware by default after the System Setup Wizard completes. You can change this behavior later. The default setting is to monitor traffic.
Acceptable Use Controls	Specifies whether or not to enable Acceptable Use Controls. If enabled, Acceptable Use Controls allow you to configure policies based on URL filtering. They also provide application visibility and control, as well as related options such as safe search enforcement. The default setting is enabled.
Reputation Filtering	Specifies whether or not to enable Web Reputation filtering for the Global Policy Group. Web Reputation Filters is a security feature that analyzes web server behavior and assigns a reputation score to a URL to determine the likelihood that it contains URL-based malware. The default setting is enabled.
Malware and Spyware Scanning	Specifies whether or not to enable malware and spyware scanning using Webroot, McAfee, or Sophos. The default setting to that all three options are enabled. If any option is enabled, also choose whether to monitor or block detected malware. The default setting is to monitor malware. You can further configure malware scanning after you finish the System Setup Wizard.
Cisco Data Security Filtering	Specifies whether or not to enable Cisco Data Security Filters. If enabled, the Cisco Data Security Filters evaluate data leaving the network and allow you to create Cisco Data Security Policies to block particular types of upload requests. The default setting is enabled.

Upstream Proxies

The web proxy can forward web traffic directly to its destination web server or use routing policies to redirect it to an external upstream proxy.

- [Upstream Proxies Task Overview, page 3-14](#)
- [Creating Proxy Groups for Upstream Proxies, page 3-14](#)

Upstream Proxies Task Overview

Task	More Information
1. Connect the external proxy upstream of the Cisco Web Security Appliance.	Connecting the Appliance, page 3-2.
2. Create and configure a proxy group for the upstream proxy.	Creating Proxy Groups for Upstream Proxies, page 3-14.
3. Create a routing policy for the proxy group to manage which traffic is routed to the upstream proxy.	Create Policies to Control Internet Requests

Creating Proxy Groups for Upstream Proxies

Step 1 Choose **Network > Upstream Proxies**.

Step 2 Click **Add Group**.

Step 3 Complete the Proxy Group settings.

Property	Description
Name	The name used to identify proxy groups on the appliance, such as in routing policies, for example.
Proxy Servers	The address, port and reconnection attempts (should a proxy not respond) for the proxy servers in the group. Rows for each proxy server can be added or deleted as required. Note You can enter the same proxy server multiple times to allow unequal load distribution among the proxies in the proxy group.

Property	Description
Load Balancing	<p>The strategy that the web proxy uses to load balance requests between multiple upstream proxies. Choose from:</p> <ul style="list-style-type: none"> • None (failover). The Web Proxy directs transactions to one external proxy in the group. It tries to connect to the proxies in the order they are listed. If one proxy cannot be reached, the Web Proxy attempts to connect to the next one in the list. • Fewest connections. The Web Proxy keeps track of how many active requests are with the different proxies in the group and it directs a transaction to the proxy currently servicing the fewest number of connections. • Hash based. Least recently used. The Web Proxy directs a transaction to the proxy that least recently received a transaction if all proxies are currently active. This setting is similar to round robin except the Web Proxy also takes into account transactions a proxy has received by being a member in a different proxy group. That is, if a proxy is listed in multiple proxy groups, the “least recently used” option is less likely to overburden that proxy. • Round robin. The Web Proxy cycles transactions equally among all proxies in the group in the listed order. <p>Note The Load Balancing option is dimmed until two or more proxies have been defined.</p>
Failure Handling	<p>Specifies the default action to take if all proxies in this group fail. Choose from:</p> <ul style="list-style-type: none"> • Connect directly. Send the requests directly to their destination servers. • Drop requests. Discard the requests without forwarding them.

Step 4 Submit and commit your changes.

Next Step.

- [Creating a Policy, page 10-5](#)

Network Interfaces

- [IP Address Versions, page 3-15](#)
- [Enabling or Changing Network Interfaces, page 3-16](#)

IP Address Versions

In Standard mode, Cisco Web Security Appliance supports IPv4 and IPv6 addresses in most cases.



Note

In Cloud Connector mode, Cisco Web Security Appliance supports IPv4 only.

A DNS server may return a result with both an IPv4 and an IPv6 address. DNS settings include an IP Address Version Preference to configure AsyncOS behavior in these cases.

Interface/Service	IPv4	IPv6	Notes
M1 interface	Required	Optional	Use of IPv6 addresses requires an IPv6 routing table that defines the default IPv6 gateway. Depending on the network, you may also need to specify a static IPv6 route in the routing table.
P1 interface	Optional	Optional	If the P1 interface has an IPv6 address configured and the appliance uses split routing (separate management and data routes), then the P1 interface cannot use the IPv6 gateway configured on the Management route. Instead, specify an IPv6 gateway for the Data routing table.
P2 interface	Optional	Optional	—
Data services	Supported	Supported	—
Control and Management Services	Supported	Partially Supported	Images, for example custom logos on end-user notification pages, require IPv4.
AnyConnect Secure Mobility (MUS)	Supported	Not Supported	—

Related Topics

- [Enabling or Changing Network Interfaces, page 3-16](#)
- [DNS Settings, page 3-31](#)

Enabling or Changing Network Interfaces

- Add or modify interface IP addresses
- Change the Layer-4 Traffic Monitor wiring type
- Enable split routing of management and data traffic

Step 1 Choose **Network > Interfaces**.

Step 2 Click **Edit Settings**.

Step 3 Configure the Interface options.

Table 3-8

Option	Description
Interfaces	<p>Modify or add new IPv4 or IPv6 Address, Netmask, and Hostname details for the M1, P1, or P2 interfaces as required.</p> <p>M1 (Management). AsyncOS requires an IPv4 address for M1. In addition to the IPv4 address, you can specify an IPv6 address. By default, the Management interface is used to administer the appliance and Web Proxy (data) monitoring. However, you can configure the M1 port for management use only.</p> <p>P1 & P2 (Data). Use an IPv4 address, IPv6 address, or use both versions. The Data interfaces are used for Web Proxy monitoring and Layer-4 Traffic Monitor blocking (optional). You can also configure these interfaces to support outbound services such as DNS, software upgrades, NTP, and traceroute data traffic.</p> <p>Note If the Management and Data interfaces are all configured, each must be assigned IP addresses on different subnets</p>
Separate Routing for Management Services	<p>Specifies whether to use M1 for management data only and to use a separate port for data traffic.</p> <p>Note When you use M1 for management traffic only, configure at least one data interface, on another subnet, for proxy traffic. Define different routes for management and data traffic.</p>
Appliance Management Services	<p>The HTTP and HTTPS ports that the appliance management services listen on. Also, specifies whether to redirect HTTP traffic to HTTPS.</p>
L4 Traffic Monitor	<p>The Layer-4 Traffic Monitor interfaces are used to configure a duplex or simplex wiring type.</p> <ul style="list-style-type: none"> • Duplex. The T1 interface receives incoming and outgoing traffic. • Simplex. T1 receives outgoing traffic and T2 receives incoming traffic.

Step 4 Submit and commit your changes.

Next Steps

- If you added an IPv6 address, add an IPv6 routing table.

Related Topics

- [Connecting the Appliance, page 3-2.](#)
- [IP Address Versions, page 3-15](#)
- [Configuring TCP/IP Traffic Routes, page 3-18.](#)

Using the P2 Data Interface for Web Proxy Data

By default, the web proxy does not listen for requests on P2, even when enabled. However, you can configure P2 to listen for web proxy data.

Before You Begin

- Enable P2 (you must also enable P1 if not already enabled) (see [Enabling or Changing Network Interfaces](#), page 3-16).

Step 1 Access the CLI.

Step 2 Use the `advancedproxyconfig -> miscellaneous` commands to access the required area

```
example.com> advancedproxyconfig
```

```
Choose a parameter group:
```

- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters

Step 3 `[> miscellaneous`

Step 4 Press **Enter** past each question until the question:

```
Do you want proxy to listen on P2?
```

Enter 'y' for this question.

Step 5 Press **Enter** past the remaining questions.

Step 6 Commit your changes.

If you enable P2 to listen for client requests using the `advancedproxyconfig > miscellaneous` CLI command, you can choose whether to use P1 or P2 for outgoing traffic. To use P1 for outgoing traffic, change the Default Route for data traffic to specify the next IP address that the P1 interface is connected to. **Related Topics**

- [Connecting the Appliance](#), page 3-2.
- [Configuring TCP/IP Traffic Routes](#), page 3-18.

Configuring TCP/IP Traffic Routes

Routes are used for determining where to send (or route) network traffic. The Web Security appliance needs to route the following kinds of traffic:

- **Data traffic.** Traffic the Web Proxy processes from end users browsing the web.
- **Management traffic.** Traffic created by managing the appliance through the web interface and traffic the appliance creates for management services, such as AsyncOS upgrades, component updates, DNS, authentication, and more.

By default, both kinds of traffic use the routes defined for all configured network interfaces. However, you can choose to split the routes (“split routing”) so that the M1 interface is only used for management traffic. When you enable split routing, data traffic only uses the routes configured for the data interfaces (P1 and P2, if configured), and management traffic uses the routes configured for all configured network interfaces.

The number of sections on the Network > Routes page is determined by whether or not split routing is enabled:

- **Separate route configuration sections for Management and Data traffic (split routing enabled).** When you use the Management interface for management traffic only (“Restrict M1 port” is enabled), then this page includes two sections to enter routes, one for management traffic and one for data traffic.
- **One route configuration section for all traffic (split routing disabled).** When you use the Management interface for both management and data traffic (“Restrict M1 port” is disabled), then this page includes one section to enter routes for all traffic that leaves the Web Security appliance, both management and data traffic.

**Note**

A route gateway must reside on the same subnet as the Management or Data interface on which it is configured. If multiple data ports are enabled, the web proxy sends out transactions on the data interface that is on the same network as the default gateway configured for data traffic.

Related Topics

- To enable split routing of management and data traffic, see [Enabling or Changing Network Interfaces, page 3-16](#)

Modifying the Default Route

-
- Step 1** Choose **Network > Routes**.
 - Step 2** Click on **Default Route** in the Management or Data table as required (or the combined Management/Data table if split routing is not enabled).
 - Step 3** In the Gateway column, enter the IP address of the computer system on the next hop of the network connected to the network interface you are editing.
 - Step 4** Submit and commit your changes.
-

Adding a Route

-
- Step 1** Choose **Network > Routes**.
 - Step 2** Click the **Add Route** button corresponding to the interface for which you are creating the route.
 - Step 3** Enter a Name, Destination Network, and Gateway.
 - Step 4** Submit and commit your changes.
-

Saving and Loading Routing Tables

-
- Step 1** Choose **Network > Routes**.
- To save a route table, click **Save Route Table** and specify where to save the file.
 - To load a saved route table, click **Load Route Table**, navigate to the file, open it, and submit and commit your changes.
-



Note

When the destination address is on the same subnet as one of the physical network interfaces, AsyncOS sends data using the network interface with the same subnet. It does not consult the routing tables.

Deleting a Route

-
- Step 1** Choose **Network > Routes**.
- Step 2** Check the checkbox in the Delete column for the appropriate route.
- Step 3** Click **Delete** and confirm.
- Step 4** Submit and commit your changes.
-

Related Topics

- [Enabling or Changing Network Interfaces, page 3-16.](#)

Configuring Transparent Redirection

Specifying a Transparent Redirection Device

Before You Begin

- Connect the appliance to a Layer-4 switch or a WCCP v2 router.

-
- Step 1** Choose **Network > Transparent Redirection**.
- Step 2** Click **Edit Device**.
- Step 3** Choose the type of device that transparently redirects traffic to the appliance from the Type drop-down list.
- Step 4** Submit and commit your changes.
- Step 5** For WCCP v2 devices, complete these additional steps:
- Configure the WCCP device using device documentation.
 - Add a WCCP service.
 - If IP spoofing is enabled on the appliance, create a second WCCP service.
-

Related Topics

- [Connecting the Appliance, page 3-2.](#)
- [Configuring WCCP Services, page 3-21.](#)

Configuring WCCP Services

A WCCP service is an appliance configuration that defines a service group to a WCCP v2 router. It includes information such as the service ID and ports used. Service groups allow a web proxy to establish connectivity with a WCCP router and to handle redirected traffic from the router.

Adding and Editing a WCCP Service

Before You Begin

- Configure the appliance to use a WCCP v2 Router (see [Specifying a Transparent Redirection Device, page 3-20](#)).

-
- Step 1** Choose **Network > Transparent Redirection**.
- Step 2** Click **Add Service**, or, to edit a WCCP service, click the name of the WCCP service in the Service Profile Name column.

Step 3 Configure the WCCP options as described:

Table 3-9


WCCP Service Option	Description
Service Profile Name	<p>The name for the WCCP service.</p> <p>Note If you leave this empty and choose a standard service (see below), the name 'web_cache' is automatically assigned here.</p>
Service	<p>The service group type for the router. Choose from:</p> <p>Standard service. This service type is assigned a fixed ID of zero, a fixed redirection method of <i>by destination port</i>, and a fixed destination port of 80. You can create one standard service only. If a standard service already exists on the appliance, this option is dimmed.</p> <p>Dynamic service. This service type allows you to define a custom ID, port numbers, and redirection and load balancing options. Enter the same parameters when creating the service on the WCCP router as you entered for the dynamic service.</p> <p>If you create a dynamic service, enter the following information:</p> <ul style="list-style-type: none"> • Service ID. Enter any number from 0 to 255 in the Dynamic Service ID field. • Port number(s). Enter up to eight port numbers for traffic to redirect in the Port Numbers field. • Redirection basis. Choose to redirect traffic based on the source or destination port. Default is destination port. <p> Note To configure Native FTP with transparent redirection and IP spoofing, choose Redirect based on source port (return path) and set the source port to 13007.</p> <ul style="list-style-type: none"> • Load balancing basis. When the network uses multiple Web Security appliances, you can choose how to distribute packets among the appliances. You can distribute packets based on the server or client address. When you choose client address, packets from a client always get distributed to the same appliance. Default is server address.
Router IP Addresses	<p>The IPv4 or IPv6 address for one or more WCCP enabled routers. Use each router's unique IP; you cannot enter a multicast address. You cannot mix IPv4 and IPv6 addresses within a service group.</p>
Router Security	<p>Specifies whether or not to require a password for this service group. If enabled, every appliance and WCCP router that uses the service group must use the same password.</p>

Table 3-9

WCCP Service Option	Description
Advanced	<p>Load-Balancing Method. This determines how the router performs load balancing of packets among multiple Web Security appliances. Choose from:</p> <ul style="list-style-type: none"> • Allow Mask Only. WCCP routers make decisions using hardware in the router. This method can increase router performance over the hash method. Not all WCCP routers support mask assignment, however. • Allow Hash Only. This method relies on a hash function to make redirection decisions. This method can be less efficient than the mask method, but may be the only option the router supports. • Allow Hash or Mask. Allows AsyncOS to negotiate a method with the router. If the router supports mask, then AsyncOS uses masking, otherwise hashing is used. <p>Mask Customization. If you select Allow Mask Only or Allow Hash or Mask, you can customize the mask or specify the number of bits:</p> <ul style="list-style-type: none"> • Custom mask (max 5 bits). You can specify the mask. The web interface displays the number of bits associated with the mask you provide. • System generated mask. You can let the system generate a mask for you. Optionally, you can specify the number of bits for the system-generated mask, up to 5 bits.
Advanced (continued)	<p>Forwarding method. This is the method by which redirected packets are transported from the router to the web proxy.</p> <p>Return Method. This is the method by which redirected packets are transported from the web proxy to the router.</p> <p>Both the forwarding and return methods use one of the following method types:</p> <ul style="list-style-type: none"> • Layer 2 (L2). This redirects traffic at layer 2 by replacing the packet's destination MAC address with the MAC address of the target web proxy. The L2 method operates at hardware level and typically offers the best performance. Not all WCCP routers support L2 forwarding, however. In addition, WCCP routers only allow L2 negotiation with a directly (physically) connected Web Security appliance. • Generic Routing Encapsulation (GRE). This method redirects traffic at layer 3 by encapsulating the IP packet with a GRE header and a redirect header. GRE operates at software level, which can impact performance. • • L2 or GRE. With this option, the appliance uses the method that the router says it supports. If both the router and appliance support L2 and GRE, the appliance uses L2. <p>If the router is not directly connected to the appliance, you must choose GRE.</p>

Step 4 Submit and commit your changes.

Creating WCCP Services for IP Spoofing

Step 1 If you have enabled IP spoofing on the web proxy, create two WCCP services. Create a standard WCCP service, or create a dynamic WCCP service that redirects traffic based on destination ports.

Step 2 Create a dynamic WCCP service that redirects traffic based on source ports.

Use the same port numbers, router IP address, and router security settings as used for the service created in [Step 1](#).



Note Cisco suggests using a service ID number from 90 to 97 for the WCCP service used for the return path (based on the source port).

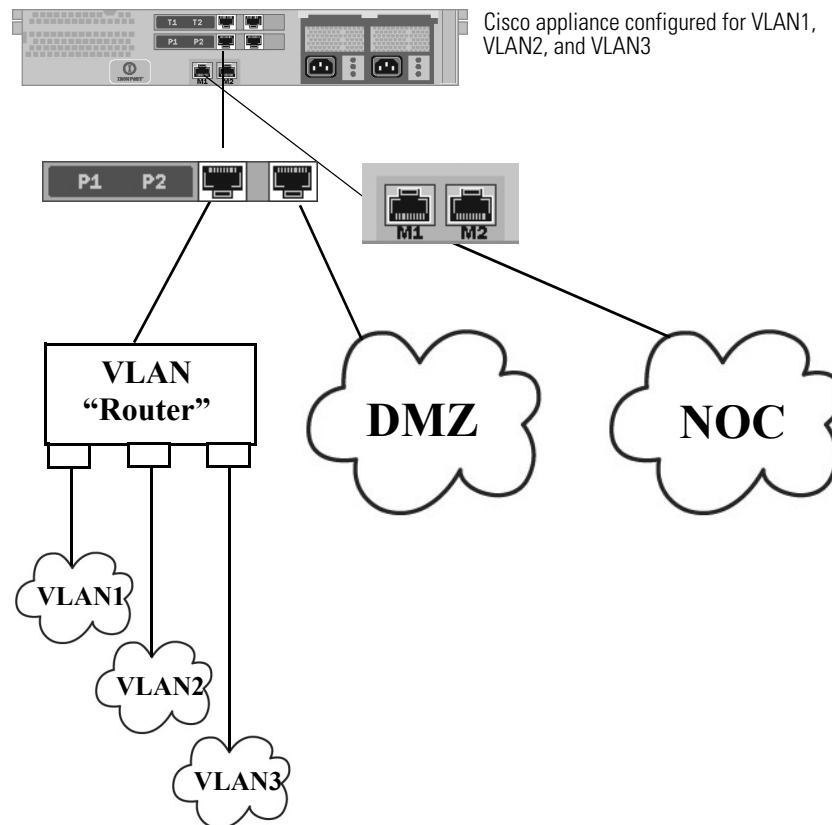
Related Topics

- [Web Proxy Cache, page 5-5](#).

Increasing Interface Capacity Using VLANs

You can configure one or more VLANs to increase the number of networks the Cisco Web Security Appliance appliance can connect to beyond the number of physical interfaces included. [Figure 3-1](#) provides an example of configuring several VLANs on the P1 interface.

Figure 3-1 Using VLANs to Increase the Number of Networks Available on the Appliance



VLANs appear as dynamic “Data Ports” labeled in the format of: “VLAN DDDD” where the “DDDD” is the ID and is an integer up to 4 digits long (VLAN 2, or VLAN 4094 for example). AsyncOS supports up to 30 VLANs.

A physical port does not need an IP address configured in order to be in a VLAN. The physical port on which a VLAN is created can have an IP that will receive non-VLAN traffic, so you can have both VLAN and non-VLAN traffic on the same interface.

VLANs can only be created on the Management and P1 data ports.

Configuring and Managing VLANs

You can create, edit and delete VLANs via the `etherconfig` command. Once created, a VLAN can be configured via the `interfaceconfig` command in the CLI.

Example 1: Creating a New VLAN

In this example, two VLANs are created (named VLAN 31 and VLAN 34) on the P1 port:

Step 1 Do not create VLANs on the T1 or T2 interfaces. Access the CLI.

Step 2 Follow the steps shown.

```
example.com> etherconfig
```

```
Choose the operation you want to perform:
```

- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.

```
[> vlan
```

```
VLAN interfaces:
```

```
Choose the operation you want to perform:
```

- NEW - Create a new VLAN.

```
[> new
```

```
VLAN ID for the interface (Ex: "34"):
```

```
[> 34
```

```
Enter the name or number of the ethernet interface you wish bind to:
```

1. Management
2. P1
3. T1
4. T2

```
[1]> 2
```

```
VLAN interfaces:
```

1. VLAN 34 (P1)

```
Choose the operation you want to perform:
```

- NEW - Create a new VLAN.

- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.

[> **new**

VLAN ID for the interface (Ex: "34"):

[> **31**

Enter the name or number of the ethernet interface you wish bind to:

1. Management
2. P1
3. T1
4. T2

[1]> **2**

VLAN interfaces:

1. VLAN 31 (P1)
2. VLAN 34 (P1)

Choose the operation you want to perform:

- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.

[>

Step 3 Commit your changes.

Example 2: Creating an IP Interface on a VLAN

In this example, a new IP interface is created on the VLAN 34 ethernet interface.

**Note**

Making changes to an interface may close your connection to the appliance.

Step 1 Access the CLI.

Step 2 Follow the steps shown.

```
example.com> interfaceconfig
```

Currently configured interfaces:

1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.

```
[> new
```

IP Address (Ex: 10.10.10.10):

```
[> 10.10.31.10
```

Ethernet interface:

1. Management
2. P1
3. VLAN 31
4. VLAN 34

```
[1]> 4
```

Netmask (Ex: "255.255.255.0" or "0xfffff000"):

```
[255.255.255.0]>
```



```
Hostname:
```

```
[> v.example.com
```

```
Currently configured interfaces:
```

1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
3. VLAN 34 (10.10.31.10 on VLAN 34: v.example.com)

```
Choose the operation you want to perform:
```

- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.

```
[>
```

```
example.com> commit
```

Step 3 Commit your changes.

Related Topics

- [Enabling or Changing Network Interfaces, page 3-16.](#)
- [Configuring TCP/IP Traffic Routes, page 3-18.](#)

Redirect Hostname and System Hostname

After running the System Setup Wizard, the System Hostname and the Redirect Hostname are the same. However, changing the system hostname using the `sethostname` command does not change the redirect hostname. Therefore the settings may have different values.

AsyncOS uses the redirect hostname for end-user notifications and acknowledgments.

The system hostname is the fully-qualified hostname used to identify the appliance in the following areas:

- The command line interface (CLI)

- System alerts
- When forming the machine NetBIOS name when the Web Security appliance joins an Active Directory domain.

The system hostname does not correspond directly to interface hostnames and is not used by clients to connect to the appliance.

Changing the Redirect Hostname

-
- Step 1** In the web user interface, navigate to **Network>Authentication**.
- Step 2** Click Edit Global Settings.
- Step 3** Enter a new value for Redirect Hostname.
-

Changing the System Hostname

-
- Step 1** Access the CLI.
- Step 2** Use the `sethostname` command to change the name of the Web Security appliance:

```
example.com> sethostname
example.com> hostname.com
example.com> commit
...
hostname.com>
```

- Step 3** Commit your changes.
-

Configuring SMTP Relay Host Settings

AsyncOS periodically sends system-generated email messages, such as notifications, alerts, and Cisco Customer Support requests. By default, AsyncOS uses information listed in the MX record on your domain to send email. However, if the appliance cannot directly reach the mail servers listed in the MX record, you must configure at least one SMTP relay host on the appliance.



Note

If the Web Security appliance cannot communicate with the mail servers listed in the MX record or any of the configured SMTP relay hosts, it cannot send email messages and it writes a message in the log files.

You can configure one or more SMTP relay hosts. When you configure multiple SMTP relay hosts, AsyncOS uses the topmost available SMTP relay host. If an SMTP relay host is unavailable, it tries to use the one below it in the list.

Configuring an SMTP Relay Host

- Step 1** Choose **Network > Internal SMTP Relay**.
- Step 2** Click **Edit Settings**.
- Step 3** Complete the Internal SMTP Relay settings.

Table 3-10

Property	Description
Relay Hostname or IP Address	The hostname or IP address to use for the SMTP relay
Port	The port for connecting to the SMTP relay. If this property is left empty, the appliance uses port 25.
Routing Table to Use for SMTP	The routing table associated with an appliance network interface, either Management or Data, to use for connecting to the SMTP relay. Choose whichever interface is on the same network as the relay system.

- Step 4** (Optional) Click **Add Row** to add additional SMTP relay hosts.
- Step 5** Submit and commit your changes.

DNS Settings

AsyncOS for Web can use the Internet root DNS servers or your own DNS servers. When using the Internet root servers, you can specify alternate servers to use for specific domains. Since an alternate DNS server applies to a single domain, it must be authoritative (provide definitive DNS records) for that domain.

- [Split DNS, page 3-31](#)
- [Clearing the DNS Cache, page 3-32](#)
- [Editing DNS Settings, page 3-32](#)

Split DNS

AsyncOS supports split DNS where internal servers are configured for specific domains and external or root DNS servers are configured for other domains. If you are using your own internal server, you can also specify exception domains and associated DNS servers.

Clearing the DNS Cache

Before You Begin

- Be aware that using this command might cause a temporary performance degradation while the cache is repopulated.

Step 1 Choose **Network > DNS**.


Step 2 Click **Clear DNS Cache**.

Editing DNS Settings

Step 1 Choose **Network > DNS**

Step 2 Click **Edit Settings**.

Step 3 Configure the DNS settings as required.

Property	Description
DNS Server(s)	<p>Use these DNS Servers. The local DNS server(s) that the appliance can use to resolve hostnames.</p> <p>Use the Internet's Root DNS Servers. You can choose to use the Internet root DNS servers for domain name service lookups when the appliance does not have access to DNS servers on your network.</p> <p>Note Internet Root DNS servers will not resolve local hostnames. If you need the appliance to resolve local hostnames you must use a local DNS server or add the appropriate static entries to the local DNS using the Command Line Interface.</p> <p>Alternate DNS servers Overrides (Optional). Authoritative DNS servers for particular domains</p>
Routing Table for DNS Traffic	Specifies which interface the DNS service will route traffic through.
IP Address Version Preference	<p>When a DNS server provides both an IPv4 and an IPv6 address, AsyncOS uses this preference to choose the IP address version.</p> <p> Note AsyncOS does not honor the version preference for transparent FTP requests.</p>
Wait Before Timing out Reverse DNS Lookups	The wait time in seconds before timing out non-responsive reverse DNS lookups.
Domain Search List	A DNS domain search list used when a request is sent to a bare hostname (with no '.' character). The domains specified will each be attempted in turn, in the order entered, to see if a DNS match for the hostname plus domain can be found.

Step 4 Submit and commit your changes.

Related Topics

- [Configuring TCP/IP Traffic Routes, page 3-18](#)
- [IP Address Versions, page 3-15](#)

Troubleshooting Connect, Install, and Configure

- [Upstream Proxy Does Not Receive Basic Credentials, page A-13](#)
- [Client Requests Fail Upstream Proxy, page A-13](#)
- [Maximum Port Entries, page A-14](#)



Connect the Appliance to a Cloud Web Security Tower

This chapter contains the following information:

- [Overview of Connect the Appliance to a Cloud Web Security Tower, page 4-1](#)
- [Documentation, page 4-4](#)
- [Deployment, page 4-5](#)
- [Configuring the Cloud Connector, page 4-5](#)
- [Directory Group Policies in the Cloud, page 4-8](#)
- [Bypassing the Cloud Proxy Server, page 4-9](#)
- [FTP and HTTPS, page 4-9](#)
- [Preventing Loss of Secure Data, page 4-10](#)
- [Cloud Connector Logs, page 4-10](#)
- [Identities and User Authentication, page 4-11](#)
- [Configuration Modes, page 4-11](#)

Overview of Connect the Appliance to a Cloud Web Security Tower

In Cloud Web Security Connector mode, the appliance connects to and routes traffic to a Cisco Cloud Web Security tower, where web security policies are enforced. The standard mode of the Web Security Appliance includes on-site web proxy services and the Layer-4 Traffic Monitor; these services are not available in Cloud Web Security Connector mode.

- [Cloud Connector versus Standard Mode, page 4-2](#)

Cloud Connector versus Standard Mode

The Web Security Appliance in Cloud Web Security Connector mode includes a subset of the features available in standard mode. Use of the features included in the Cloud Connector subset is the same in both modes.

Menu	Available in Cloud Connector Mode	Available in Standard Mode
Reporting	System Status	System Status Overview Users Web Sites URL Categories Application Visibility Anti-Malware Client Malware Risk Web Reputation Filters Layer-4 Traffic Monitor Reports by User Location Web Tracking System Capacity Scheduled Reports Archived Reports
Web Security Manager	Identities Cloud Routing Policies External Data Loss Prevention Custom URL Categories	Identities Cloud Routing Policies External Data Loss Prevention Custom URL Categories Policies Decryption Policies Routing Policies Access Policies Overall Bandwidth Limits Cisco Data Security Outbound Malware Scanning Defined Time Ranges Bypass Settings Layer-4 Traffic Monitor

Menu	Available in Cloud Connector Mode	Available in Standard Mode
Security Services	Web Proxy	Web Proxy FTP Proxy HTTPS Proxy PAC File Hosting Identity Provider for SaaS Acceptable Use Controls Anti-Malware and Reputation Data Transfer Filters AnyConnect Secure Mobility End-User Notification Layer-4 Traffic Monitor SensorBase Reporting

Menu	Available in Cloud Connector Mode	Available in Standard Mode
Network	Interfaces Transparent Redirection Routes DNS Internal SMTP Relay Authentication External DLP Servers Cloud Connector	Interfaces Transparent Redirection Routes DNS Internal SMTP Relay Authentication External DLP Servers Upstream Proxy
System Administration	Users Alerts Log Subscriptions Network Access Time Zone Time Settings Configuration Summary Configuration File Feature Keys Upgrade and Update Settings System Upgrade System Setup Wizard	Users Alerts Log Subscriptions Network Access Time Zone Time Settings Configuration Summary Configuration File Feature Keys Upgrade and Update Settings System Upgrade System Setup Wizard Policy Trace Return Addresses Feature Keys Settings Next Steps

Documentation

This chapter links to locations within this User Guide that provide information about some of the major features of the Web Security Appliance that are common to both standard mode and Cloud Web Security Connector mode. With the exception of Cloud Connector configuration settings and information about sending directory groups to the cloud, relevant information is in other locations throughout this guide.

This chapter includes information about configuring the Cloud Web Security Connector that is not applicable in standard mode.

This guide does not include information about the Cisco Cloud Web Security product. Cisco Cloud Web Security documentation is available on Cisco.com.

Related topics

- http://www.cisco.com/en/US/products/ps11720/tsd_products_support_series_home.html

Deployment

Deployment of the appliance is the same in both standard and Cloud Security mode except that on-site web proxy services and Layer-4 Traffic Monitor services are not available in Cloud Web Security Connector mode.

You can deploy the Cloud Web Security Connector in either explicit forward mode or in transparent mode.

Related topics

- [Chapter 3, “Connect, Install, and Configure”](#)

Configuring the Cloud Connector

Step 1. Access the Web Interface for the Web Security Appliance

Step 1 Enter the IPv4 address of the Web Security appliance in an internet browser.

The first time you run the System Setup Wizard, use the default IPv4 address:

```
https://192.168.42.42:8443
```

-or-

```
http://192.168.42.42:8080
```

where 192.168.42.42 is the default IPv4 address, and 8080 is the default admin port setting for HTTP, and 8443 is default admin port for HTTPS.

Step 2. Accept the License Agreement and Begin Setup.

Step 1 Navigate to **System Administration>System Setup Wizard**.

Step 2 Accept the terms of the license agreement.

Step 3 Click **Begin Setup**.

Step 3. Configure System Settings:

Setting	Description
Default System Hostname	The fully-qualified hostname for the Web Security appliance.
DNS Server(s)	The Internet root DNS servers for domain name service lookups.
NTP Server	A server with which to synchronize the system clock. The default is time.ironport.com.
Time Zone	Sets the time zone on the appliance so that timestamps in message headers and log files are correct.

Related topics

- [DNS Settings, page 3-31](#)

Step 4. Set the Appliance Mode

Step 1 Select Cloud Web Security Connector.

Step 5. Configure Cloud Connector Settings

Setting	Description
Cloud Web Security Proxy Servers	The address of the Cloud Proxy Server (CPS), for example, proxy1743.scansafe.net.
Failure Handling	If AsyncOS fails to connect to a Cloud Web Security tower, either Connect directly to the internet or Drop requests .
Cloud Web Security Authorization Scheme	Method for authorizing transactions: <ul style="list-style-type: none"> • Web Security Appliance public facing IPv4 address • Authorization key included with each transaction. You can generate an authorization key within the Cisco Cloud Web Security Portal.



Note

You can return to these settings later by navigating to **Network>Cloud Connector**.

Related topics

- [Preventing Loss of Secure Data, page 4-10](#)

- [Sending Directory Groups to the Cloud, page 4-8](#)

Step 6. Configure Network Interfaces and Wiring

Setting	Description
Ethernet Port	If you configure the M1 interface for management traffic only, you must configure the P1 interface for data traffic. However, you can configure the P1 interface even when the M1 interface is used for both management and data traffic.
IP Address	The IPv4 address to use to manage the Web Security appliance.
Network Mask	The network mask to use when managing the Web Security appliance on this network interface.
Hostname	The hostname to use when managing the Web Security appliance on this network interface.

Related topics

- [Network Interfaces, page 3-15](#)

Step 7. Configure Routes for Management and Data Traffic

Setting	Description
Default Gateway	The default gateway IPv4 address to use for the traffic through the Management and/or Data interface.
Name	A name used to identify the static route.
Internal Network	The IPv4 address for this route's destination on the network.
Internal Gateway	The gateway IPv4 address for this route. A route gateway must reside on the same subnet as the Management or Data interface on which it is configured.

Related topics

- [Configuring TCP/IP Traffic Routes, page 3-18](#)

Step 8. Configure Transparent Connection Settings

By default, the Cloud Connector is deployed in transparent mode, which requires a connection to a Layer-4 switch or a version 2 WCCP router.

Setting	Description
Layer-4 Switch or No Device	<ul style="list-style-type: none"> • The Web Security appliance is connected to a layer 4 switch. or <ul style="list-style-type: none"> • You will deploy the Cloud Connector in explicit forward mode.
WCCP v2 Router	The Web Security appliance is connected to a version 2 WCCP capable router. Note: A password can contain up to seven characters and is optional.

Related topics

- [Configuring Transparent Redirection, page 3-20](#)

Step 9. Configure Administrative Settings

Setting	Description
Administrator Password	A password to access the Web Security appliance. The password must be six characters or more.
Email system alerts to	An email address to which the appliance sends alerts.
Send Email via SMTP Relay Host	(Optional) A hostname or address for an SMTP relay host that AsyncOS uses for sending system generated email messages. The default SMTP relay host is the mail servers listed in the MX record. The default port number is 25.
AutoSupport	The appliance can send system alerts and weekly status report to Cisco Customer Support.

Related topics

- [Managing Alerts, page 21-13](#)
- [Configuring SMTP Relay Host Settings, page 3-30](#)

Step 10. Review and Install

-
- Step 1** Review the installation.
- Step 2** Click **Previous** to go back and make changes.
- Step 3** Click **Install This Configuration** to continue with the information you provided.
-

Directory Group Policies in the Cloud

You can use Cisco Cloud Web Security to control web access based on directory groups. When traffic to Cisco Cloud Web Security is being routed through a Web Security Appliance in Cloud Connector mode, Cisco Cloud Web Security needs to receive the directory-group information with the transactions from the Cloud Connector so it can apply the group-based cloud policies. You can configure the Cloud Connector to send specific directory groups to the cloud for this purpose.

- [Sending Directory Groups to the Cloud, page 4-8](#)

Sending Directory Groups to the Cloud

Before you begin

- Add an authentication realm to the Web Security Appliance configuration.

-
- Step 1** Navigate to **Network>Cloud Connector**.
- Step 2** In the **Cloud Policy Directory Groups** area, click **Edit Groups**.
- Step 3** Select the groups for which you have created Cloud Policies within Cisco Cloud Web Security.
- Step 4** Click **Add**.
- Step 5** Click **Done** and Commit your changes.
-

Related information

- [About Authentication Realms, page 6-3](#)

Bypassing the Cloud Proxy Server

Cloud routing policies allow you to route web traffic to either Cisco Cloud Web Security towers or directly to the Internet based on these characteristics:

- Identity
- Proxy Port
- Subnet
- URL Category
- User Agent

The process of creating cloud routing policies in Cloud Connector mode is identical to the process of creating routing policies using the standard mode.

Related topics

- [Creating a Policy, page 10-5](#)

FTP and HTTPS

The Web Security appliance in Cloud Connector mode does not fully support FTP or HTTPS.

- [FTP, page 4-9](#)
- [HTTPS, page 4-9](#)

FTP

FTP is not supported by the Cloud Connector. AsyncOS drops native FTP traffic when the appliance is configured for Cloud Connector.

FTP over HTTP is supported in Cloud Connector mode.

HTTPS

The Cloud Connector does not support decryption. It passes through HTTPS traffic without decrypting.

Because the Cloud Connector does not support decryption, AsyncOS generally does not have access to information in the client headers of HTTPS traffic. Therefore, AsyncOS generally cannot enforce routing policies that rely on information in encrypted headers. This is always the case for transparent HTTPS transactions. For example, for transparent HTTPS transactions, AsyncOS does not have access to the port number in the HTTPS client header and therefore it cannot match a routing policy based on port number. In this case, AsyncOS uses the default routing policy.

There are two exceptions for explicit HTTPS transactions. AsyncOS has access to the following information for explicit HTTPS transactions:

- URL
- Destination port number

For explicit HTTPS transactions, it is possible to match a routing policy based on URL or port number.

Preventing Loss of Secure Data

You can integrate the Cloud Connector with external Data Loss Prevention servers through **Network>External DLP Servers**.

Related topics

- [Chapter 15, “Prevent Loss of Sensitive Data”](#)

Cloud Connector Logs

The Cloud Connector Logs provides useful information for troubleshooting problems with the Cloud Connector, for example, authenticated users and groups, the Cloud header, and the authorization key.

- [Subscribing to the Cloud Connector Logs, page 4-10](#)

Subscribing to the Cloud Connector Logs

-
- Step 1** Navigate to **System Administration>Log Subscriptions**.
 - Step 2** Select **Cloud Connector Logs** from the **Log Type** menu.
 - Step 3** Type a name in the **Log Name** field.
 - Step 4** Set the log level.
 - Step 5** Submit and Commit your changes.
-

Related topics

- [Chapter 20, “Monitor System Activity Through Logs”](#)



Tip

Go to whoami.scansafe.net to view the configured group names, user names, and IP addresses.

Identities and User Authentication

The Cloud Web Security Connector supports basic authentication and NTLM. You can also bypass authentication for certain destinations. With the exception of Kerberos, Authentication works the same throughout the Web Security Appliance, whether in standard configuration or Cloud Connector configuration. AsyncOS does not support Kerberos when the appliance is configured in Cloud Connector mode.

- [Guest Access for Unauthenticated Users, page 4-11](#)

**Note**

Identities based on User Agent or Destination URL are not supported for HTTPS traffic.

Related topics

- [Chapter 7, “Classify End-Users and Client Software”](#)
- [Chapter 6, “Acquire End-User Credentials”](#)

Guest Access for Unauthenticated Users

If the Web Security appliance is configured to provide guest access for unauthenticated users, in Cloud Connector mode, AsyncOS assigns guest users to the group, `__GUEST_GROUP__`, and sends that information to Cisco Cloud Web Security. Use Identities to provide guest access to unauthenticated users. Use Cisco Cloud Web Security policies to control these guest users.

Related topics

- [Granting Guest Access After Failed Authentication, page 6-20](#)

Configuration Modes

You can switch between Cloud Connector and Standard modes using the System Setup Wizard.

- [Switching to Cloud Connector Mode, page 4-11](#)

Switching to Cloud Connector Mode

Switching to Cloud Connector Mode

-
- | | |
|---------------|--|
| Step 1 | Select System Administration>System Setup Wizard . |
| Step 2 | Accept the license agreement. |
| Step 3 | Select Cloud Web Security Connector in the Appliance Mode section. |
| Step 4 | Continue configuring the Cloud Connector as described later in this chapter. |
-

Related topics

- [Configuring the Cloud Connector, page 4-5](#)



Intercepting Web Requests

- [Overview of Intercepting Web Requests, page 5-1.](#)
- [Tasks for Intercepting Web Requests, page 5-2.](#)
- [Best Practices for Intercepting Web Requests, page 5-2.](#)
- [Web Proxy Options for Intercepting Web Requests, page 5-3.](#)
- [Client Options for Redirecting Web Requests, page 5-11.](#)
- [Using PAC Files with Client Applications, page 5-11.](#)
- [FTP Proxy Services, page 5-14.](#)
- [SOCKS Proxy Services, page 5-16](#)

Overview of Intercepting Web Requests

The Web Security appliance intercepts requests that are forwarded to it by clients or other devices over the network.

The appliance works in conjunction with other network devices to intercept traffic. These may be ordinary switches, transparent redirection devices, network taps, and other proxy servers or Web Security appliances.

Tasks for Intercepting Web Requests

Steps	Task	Links to Related Topics and Procedures
1.	Review best practices.	<ul style="list-style-type: none"> • Best Practices for Intercepting Web Requests, page 5-2
2.	(Optional) Perform follow up networking tasks: <ul style="list-style-type: none"> • Connect and configure upstream proxies. • Configure network interface ports. • Configure transparent redirection devices. • Configure TCP/IP routes. • Configure VLANs. 	<ul style="list-style-type: none"> • Upstream Proxies, page 3-13 • Network Interfaces, page 3-15 • Configuring Transparent Redirection, page 3-20 • Configuring TCP/IP Traffic Routes, page 3-18 • Increasing Interface Capacity Using VLANs, page 3-24
3.	(Optional) Perform follow up Web Proxy tasks: <ul style="list-style-type: none"> • Configure the web proxy to operate in either Forward or Transparent mode. • Decide if additional services are needed for the protocol types you want to intercept • Configure IP spoofing. • Manage the web proxy cache. • Use custom web request headers. • Bypass the proxy for some requests. 	<ul style="list-style-type: none"> • Web Proxy Options for Intercepting Web Requests, page 5-3 • Configuring Web Proxy Settings, page 5-3 • Web Proxy Options for Intercepting Web Requests, page 5-3 • Web Proxy Cache, page 5-5 • Web Proxy IP Spoofing, page 5-8 • Web Proxy Bypassing, page 5-10
4.	Perform client tasks: <ul style="list-style-type: none"> • Decide how clients should redirect requests to the web proxy. • Configure clients and client resources. 	<ul style="list-style-type: none"> • Client Options for Redirecting Web Requests, page 5-11 • Using PAC Files with Client Applications, page 5-11
5.	(Optional) Enable and Configure the FTP proxy.	<ul style="list-style-type: none"> • FTP Proxy Services, page 5-14

Best Practices for Intercepting Web Requests

- Enable only the proxy services you require.
- Use the same forwarding and return method (either L2 or GRE) for all WCCP services defined in the Web Security appliance. This allows the proxy bypass list to work consistently.
- Ensure that users cannot access PAC files from outside the corporate network. This allows your mobile workers to use the web proxy when they are on the corporate network and to connect directly to web servers at other times.
- Allow a web proxy to accept X-Forwarded-For headers from trustworthy downstream proxies or load balancers only.
- Leave the web proxy in the default transparent mode, even if initially using only explicit forwarding. Transparent mode also accepts explicitly forwarded requests.

Web Proxy Options for Intercepting Web Requests

By itself, the Web Proxy can intercept web requests that use HTTP (including FTP over HTTP) and HTTPS. Additional proxy modules are available to enhance protocol management:

- **FTP Proxy.** The FTP Proxy allows the interception of native FTP traffic (rather than just FTP traffic that has been encoded within HTTP).
- **HTTPS Proxy.** The HTTPS proxy supports the decryption of HTTPS traffic and allows the web proxy to pass unencrypted HTTPS requests on to policies for content analysis.



Note When in transparent mode, the Web Proxy drops all transparently redirected HTTPS requests if the HTTPS proxy is not enabled. No log entries are created for dropped transparently redirected HTTPS requests.

- **SOCKS Proxy.** The SOCKS proxy allows the interception of SOCKS traffic.

Each of these additional proxies requires the Web Proxy in order to function. You cannot enable them if you disable the Web Proxy.



Note The Web proxy is enabled by default. All other proxies are disabled by default.

Related Topics

- [FTP Proxy Services, page 5-14.](#)
- [SOCKS Proxy Services, page 5-16](#)

Configuring Web Proxy Settings

Before You Begin

- Enable the web proxy.



-
- Step 1** Choose **Security Services > Web Proxy**.
- Step 2** Click **Edit Settings**.
- Step 3** Configure the basic web proxy settings as required.

Property	Description
HTTP Ports to Proxy	The ports that the web Proxy will listen on for HTTP connections
Caching	Specifies whether to enable or disable Web Proxy caching. The web proxy caches data to increase performance.

Property	Description
Proxy mode	<ul style="list-style-type: none"> • Forward — Allow the client browser to name the internet target. Requires individual configuration of each web browser to use the web proxy. The web proxy can intercept only explicitly forwarded web requests in this mode. • Transparent (Recommended) — Allow the web proxy to name the internet target. The web proxy can intercept both transparent and explicitly forwarded web requests in this mode.
IP Spoofing	<ul style="list-style-type: none"> • IP Spoofing disabled — The web proxy changes the request source IP address to match its own address to increase security. • IP Spoofing disabled — The web proxy retains the source address so that it appears to originate from the source client rather than from the Web Security appliance.

Step 4 Complete the advanced web proxy settings as required.

Property	Description
Persistent Connection Timeout	<p>The maximum time in seconds the web proxy keeps open a connection to a client or server after a transaction has been completed and no further activity is detected.</p> <ul style="list-style-type: none"> • Client side. The timeout value for connections to clients. • Server side. The timeout value for connections to servers. <p>If you increase these values connections will remain open longer and reduce the overhead used to open and close connections repeatedly. However, you also reduce the ability of the Web Proxy to open new connections if the maximum number of simultaneous persistent connections has been reached.</p> <p>Cisco recommends keeping the default values.</p>
In-Use Connection Timeout	<p>The maximum time in seconds that the web proxy waits for more data from an idle client or server when the current transaction has not yet been completed.</p> <ul style="list-style-type: none"> • Client side. The timeout value for connections to clients. • Server side. The timeout value for connections to servers.
Simultaneous Persistent Connections (Server Maximum Number)	<p>The maximum number of connections (sockets) the Web Proxy keeps open with servers.</p>

Generate Headers	<p>Generate and add headers that encode information about the request.</p> <ul style="list-style-type: none"> • X-Forwarded-For headers encode the IP address of the client from which an HTTP request originated. <hr/> <p> Note To turn header forwarding on or off, use the CLI <code>advancedproxyconfig</code> command, Miscellaneous option, “Do you want to pass HTTP X-Forwarded-For headers?”</p> <hr/> <p> Note Using an explicit forward upstream proxy to manage user authentication or access control with proxy authentication requires forwarding of these headers.</p> <hr/> <ul style="list-style-type: none"> • Request Side VIA headers encode the proxies through which the request passed on its way from the client to the server. • Response Side VIA headers encode the proxies through which the request passed on its way from the server to the client.
Use Received Headers	<p>Allows a Web proxy deployed as an upstream proxy to identify clients using X-Forwarded-For headers send by downstream proxies. The Web Proxy will not accept the IP address in a X-Forwarded-For header from a source that is not included in this list.</p> <p>If enabled, requires the IP address of a downstream proxy or load balancer (you cannot enter subnets or hostnames).</p>

Step 5 Submit and commit your changes.

Related Topics

- [Web Proxy Cache, page 5-5.](#)
- [Configuring Transparent Redirection, page 3-20](#)

Web Proxy Cache

The web proxy caches data to increase performance. AsyncOS includes predefined caching modes that range from safe to aggressive and also allows you to customize caching. You can also exclude specific URLs from being cached, either by removing them from the cache or by configuring the cache to ignore them.

Clearing the Web Proxy Cache

- Step 1** Choose **Security Services > Web Proxy**.
- Step 2** Click **Clear Cache** and confirm your action.

Removing URLs from the Web Proxy Cache

Step 1 Access the CLI.

Step 2 Use the `webcache -> evict` commands to access the required caching area:

```
vm10wsa0019.qa> webcache
```

```
Choose the operation you want to perform:
```

```
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict
```

```
Enter the URL to be removed from the cache.
```

```
[]>
```

Step 3 Enter the URL to be removed from the cache:



Note If you do not include a protocol in the URL, `http://` will be prepended to it (e.g. `www.cisco.com` will become `http://www.cisco.com`)

Specifying Domains or URLs that the Web Proxy never Cache

Step 1 Access the CLI.

Step 2 Use the `webcache -> ignore` commands to access the required submenus:

```
example.com> webcache
```

```
Choose the operation you want to perform:
```

```
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore
```

```
Choose the operation you want to perform:
```

```
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

Step 3 Enter the address type you wish to manage: domains or urls.

```
[]> urls
```

```
Manage url entries:
```

```
Choose the operation you want to perform:
```

```
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```


Step 4 Choose to add new entries:

```
[ ]> add
```

Enter new url values; one on each line; an empty line to finish
[]>

Step 5 Enter domain or url values, for example:

```
Enter new url values; one on each line; an empty line to finish  
[ ]> www.example1.com
```

Enter new url values; one on each line; an empty line to finish
[]>



Note You can include embedded regular expression (regex) characters in the domain or URL you specify.

Step 6 When finished entering values, press **Enter** until you return to the main command interface.

Step 7 Commit your changes.

Choosing The Web Proxy Cache Mode

Step 1 Access the CLI.

Step 2 Use the `advancedproxyconfig -> caching` commands to access the required submenus:

```
example.com> advancedproxyconfig
```

Choose a parameter group:

- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters

```
[ ]> caching
```

Enter values for the caching options:

The following predefined choices exist for configuring advanced caching options:

1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode

Please select from one of the above choices:

```
[2]>
```

Step 3 Enter a number corresponding to the web proxy cache settings you require:

Entry	Mode	Description
1	Safe	The least caching and the most adherence to RFC #2616 compared to the other modes.
2	Optimized	Moderate caching and moderate adherence to RFC #2616. Compared to safe mode, in optimized mode the Web Proxy caches objects when no caching time is specified when a Last-Modified header is present. The Web Proxy caches negative responses.
3	Aggressive	The most caching and the least adherence to RFC #2616. Compared to optimized mode, aggressive mode caches authenticated content, ETag mismatches, and content without a Last-Modified header. The Web Proxy ignores the no-cache parameter.
4	Customized mode	Configure each parameter individually.

Step 4 If you chose option 4 (Customized mode), enter values (or leave at the default values) for each of the custom settings.

Step 5 Press **Enter** until you return to the main command interface.

Step 6 Commit your changes.

Related Topics

- [Web Proxy Cache, page 5-5.](#)

Web Proxy IP Spoofing

When the web proxy forwards a request, it changes the request source IP address to match its own address by default. This increases security, but you can change this behavior by implementing IP spoofing, so that requests retain their source address and appear to originate from the source client rather than from the Web Security appliance.

IP spoofing works for transparent and explicitly forwarded traffic. When the Web Proxy is deployed in transparent mode, you have the choice to enable IP spoofing for transparently redirected connections only or for all connections (transparently redirected and explicitly forwarded). If explicitly forwarded connections use IP spoofing, you should ensure that you have appropriate network devices to route return packets back to the Web Security appliance.

When IP spoofing is enabled and the appliance is connected to a WCCP router, you must configure two WCCP services: one based on source ports and one based on destination ports.

Related Topics

- [Configuring Web Proxy Settings, page 5-3.](#)
- [Configuring WCCP Services, page 3-21.](#)

Web Proxy Custom Headers

You can add custom headers to specific outgoing transactions to request special handling from destination servers. For example, if you have a relationship with YouTube for Schools, you can use a custom header to identify transaction requests to YouTube.com as coming from your network and as requiring special handling.

Adding Custom Headers To Web Requests

Step 1 Access the CLI.

Step 2 Use the `advancedproxyconfig -> customheaders` commands to access the required submenus:

```
example.com> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> customheaders

Currently defined custom headers:

Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
- EDIT - Edit entries
[]>
```

Step 3 Enter the required subcommand as follows:

Option	Description
Delete	Deletes the custom header you identify. Identify the header to delete using the number associated with the header in the list returned by the command.
New	Creates the header you provide for use with the domain or domains you specify. Example header: X-YouTube-Edu-Filter: ABCD1234567890abcdef (The value in this case is a unique key provided by YouTube.) Example domain: youtube.com
Edit	Replaces an existing header with one you specify. Identify the header to delete using the number associated with the header in the list returned by the command.

Step 4 Press **Enter** until you return to the main command interface.

Step 5 Commit your changes.

Web Proxy Bypassing

- [Web Proxy Bypassing for Web Requests, page 5-10](#)
- [Configuring Web Proxy Bypassing for Web Requests, page 5-10](#)
- [Configuring Web Proxy Bypassing for Applications, page 5-10](#)

Web Proxy Bypassing for Web Requests

You can configure the Web Security appliance so that transparent requests from particular clients, or to particular destinations, bypass the Web Proxy.

Bypassing the web proxy allows you to:

- Prevent interference with non-HTTP-compliant (or proprietary) protocols that use HTTP ports but do not work properly when they connect to a proxy server.
- Ensure that traffic from a particular machine inside the network, such as a malware test machine, bypasses the Web Proxy and all its built-in security protection.

Bypassing only works for requests that are transparently redirected to the web proxy. The web proxy processes all requests that clients explicitly forward to it, whether the proxy is in transparent or forward mode.

Configuring Web Proxy Bypassing for Web Requests

- Step 1** Choose **Web Security Manager > Bypass Settings**.
- Step 2** Click **Edit Bypass Settings**.
- Step 3** Enter the addresses for which you wish to bypass the web proxy.
- Step 4** Submit and commit your changes.
-

Configuring Web Proxy Bypassing for Applications

- Step 1** Choose **Web Security Manager > Bypass Settings**.
- Step 2** Click **Edit Application Bypass Settings**.
- Step 3** Select the application(s) you wish to bypass scanning for.
- Step 4** Submit and commit your changes.
-

Web Proxy Usage Agreement

You can configure the Web Security appliance to inform users that it is filtering and monitoring their web activity. The appliance does this by displaying an end-user acknowledgment page when a user first accesses a browser after a certain period of time. When the end-user acknowledgment page appears, users must click a link to access the original site requested or any other website.

Related Topics

- [Notify End-Users of Proxy Actions](#)

Client Options for Redirecting Web Requests

If you choose to have clients explicitly forward requests to the web proxy, you must also decide how to configure the clients to do this. Choose from the following methods:

- **Configure Clients Using Explicit Settings.** Configure clients with the web proxy hostname and port number. See individual client documentation for details on how to do this.



Note The web proxy port uses port numbers 80 and 3128 by default. Clients can use either port.

- **Configure Clients Using a Proxy Auto-Config (PAC) File.** PAC files provide clients with instructions on where to direct web requests. This options allows you to centrally manage subsequent changes to the proxy details.

If you choose to use PAC files, you must also choose where to store them and how clients will find them.

Related Topics

- [Using PAC Files with Client Applications, page 5-11.](#)

Using PAC Files with Client Applications

Options For Publishing Proxy Auto-Config (PAC) Files

You must publish PAC files where clients can access them. Valid locations are:

- **Web servers.**
- **Web Security appliances.** You can place PAC files on a Web Security appliance, which appears to clients as a web browser. The appliance also offers additional options to manage PAC files, including the ability to service requests that use different hostnames, ports, and file names.
- **Local machines.** You can place the PAC file locally on a client's hard disk. Cisco does not recommend this as a general solution, and it is not suited to automatic PAC file detection methods, but it can be useful for testing.

Related Topics

- [Hosting PAC Files on the Web Security Appliance, page 5-12.](#)
- [Specifying PAC Files in Client Applications, page 5-13.](#)

Client Options For Finding Proxy Auto-Config (PAC) Files

If you choose to use PAC files for your clients, you must also choose how clients will find the PAC files. You have two options:

- **Configure client with the PAC file location.** Configure the client with a URL that specifically points to the PAC file.
- **Configure clients to detect the PAC file location automatically.** Configure clients to find PAC files automatically using the WPAD protocol along with DHCP or DNS.

Automatic PAC File Detection

WPAD is a protocol that allows the browser determine the location of a PAC file using DHCP and DNS.

- **To use WPAD with DHCP,** you must set up option 252 on the DHCP server's with the url of the PAC file location. Not all browsers support DHCP, however.
- **To use WPAD with DNS,** you must configure a DNS record to point to the PAC file's host server.

You can configure either or both options. WPAD will first try to find PAC files using DHCP, and if it cannot, it will then try DNS.

Related Topics

- [Detecting the PAC File Automatically in Clients, page 5-13](#)

Hosting PAC Files on the Web Security Appliance

Step 1 Choose **Security Services > PAC File Hosting**

Step 2 Click **Enable and Edit Settings**.

Step 3 (Optional) Complete the following basic settings:

Option	Description
PAC Server Ports	The ports that the Web Security appliance will use to listen for PAC file requests.
PAC File Expiration	Allows the PAC file to expire after a specified number of minutes in the browser's cache.

Step 4 Click **Browse** in the PAC Files section and select a PAC file from your local machine for upload to the Web Security appliance.



Note If the file you select is called `default.pac`, you do not have to specify the file name when configuring its location in a browser. The Web Security appliance looks for a file called `default.pac` if no name is specified.

Step 5 Click **Upload** to upload the PAC file selected in step 4 to the Web Security appliance.

- Step 6** (Optional) In the Hostnames for Serving PAC Files Directly section, configure hostnames and associated file names for PAC file requests that do not include a port number:

Option	Description
Hostname	The hostname that the PAC file request must include if the Web Security appliance is to service the request. As the request does not include a port number, it will be processed through the Web Proxy HTTP ports (e.g. port 80) and must be distinguishable as a PAC file request through this hostname-value.
Default PAC File for "Get/" Request through Proxy Port	The PAC file name that will be associated with the hostname on the same row. Request to the hostname will return the PAC file specified here. Only PAC files that have been uploaded are available for selection.
Add Row	Adds another row to specify additional hostnames and PAC file names.

- Step 7** Submit and commit your changes.

Specifying PAC Files in Client Applications

- [Configuring a PAC File Location Manually in Clients, page 5-13](#)
- [Detecting the PAC File Automatically in Clients, page 5-13](#)

Configuring a PAC File Location Manually in Clients

- Step 1** Create and publish a PAC file.

- Step 2** Enter a URL in your browser's PAC file configuration area that points to the PAC file location.

The following are valid URL formats if the Web Security appliance is hosting the PAC file:

```
http://server_address[.domain][:port][/filename] | http://WSAHostname[/filename]
```

where *WSAHostname* is the **hostname** value configured when hosting the PAC file on a Web Security appliance. Otherwise the URL format will depend on the storage location and, in some cases, on the client.

Related Topics

- [Hosting PAC Files on the Web Security Appliance, page 5-12.](#)

Detecting the PAC File Automatically in Clients

- Step 1** Create a PAC file called `wpad.dat` and publish it to a web server or Web Security appliance (the file must be placed in a web server's root folder if you intend using WPAD with DNS).

- Step 2** Configure the web server to set up `.dat` files with the following MIME type:

```
application/x-ns-proxy-autoconfig
```



Note A Web Security appliance does this for you automatically.

- Step 3** To support DNS lookup, create an internally resolvable DNS name beginning with 'wpad' (for example, wpad.example.com) and associate it with the IP address of the server hosting the wpad.dat file.
- Step 4** To support DHCP lookup, configure your DHCP server's option 252 with the url of the wpad.dat file location (for example: "http://wpad.example.com/wpad.dat"). The URL can use any valid host address, including an IP address, and does not require a specific DNS entry.
-

Related Topics

- [Using PAC Files with Client Applications, page 5-11.](#)
- [Hosting PAC Files on the Web Security Appliance, page 5-12.](#)

FTP Proxy Services

- [Overview of FTP Proxy Services, page 5-14](#)
- [Enabling and Configuring the FTP Proxy, page 5-14](#)

Overview of FTP Proxy Services

The web proxy can intercept two types of FTP requests:

- **Native FTP.** Native FTP requests are generated by dedicated FTP clients (or by browsers using built-in FTP clients). Requires the FTP proxy.
- **FTP over HTTP.** Browsers sometimes encode FTP requests inside HTTP requests, rather than using native FTP. Does not require the FTP proxy.

Related Topics

- [Enabling and Configuring the FTP Proxy, page 5-14.](#)
- [Configuring FTP Notification Messages, page 16-13.](#)

Enabling and Configuring the FTP Proxy

- Step 1** Choose **Security Services > FTP Proxy**.
- Step 2** Click **Enable and Edit Settings** (if the only available option is **Edit Settings** then the FTP proxy is already enabled).

Step 3 (Optional) Configure the basic FTP Proxy settings.

Property	Description
Proxy Listening Port	The port that the FTP Proxy will listen to for FTP control connections. Clients should use this port when configuring an FTP proxy (not as the port for connecting to FTP servers, which normally use port 21).
Caching	Whether or not data connections from anonymous users are cached. Note Data from non-anonymous users is never cached.
Server Side IP Spoofing	Allows the FTP Proxy to imitate the FTP server's IP address. This supports FTP clients that do not allow transactions when the IP address is different for the control and data connections.
Authentication Format	Allows a choice of authentication format the FTP Proxy can use when communicating with FTP clients.
Passive Mode Data Port Range	The range of TCP ports that FTP clients should use to establish a data connection with the FTP Proxy for passive mode connections.
Active Mode Data Port Range	The range of TCP ports FTP servers should use to establish a data connection with the FTP Proxy for active mode connections. This setting applies to both native FTP and FTP over HTTP connections. Increasing the port range accommodates more requests from the same FTP server. Because of the TCP session TIME-WAIT delay (usually a few minutes), a port does not become available again for the <i>same</i> FTP server immediately after being used. As a result, any given FTP server cannot connect to the FTP Proxy in active mode more than <i>n</i> times in a short period of time, where <i>n</i> is the number of ports specified in this field.
Welcome Banner	The welcome banner that appears in FTP clients during connection. Choose from: <ul style="list-style-type: none"> • FTP server message. The message will be provided by the destination FTP server. This option is only available when the web proxy is configured for transparent mode, and only applies for transparent connections. • Custom message. When selected, this custom message is displayed for all native FTP connections. When not selected, this is still used for explicit forward native FTP connections.

Step 4 (Optional) Configure the advanced FTP Proxy settings:

Property	Description
----------	-------------

Control Connection Timeouts	<p>The maximum number of seconds the FTP Proxy waits for more communication in the control connection from an idle FTP client or FTP server when the current transaction has not been completed.</p> <ul style="list-style-type: none"> • Client side. The timeout value for control connections to idle FTP clients. • Server side. The timeout value for control connections to idle FTP servers.
Data Connection Timeouts	<p>How long the FTP Proxy waits for more communication in the data connection from an idle FTP client or FTP server when the current transaction has not been completed.</p> <ul style="list-style-type: none"> • Client side. The timeout value for data connections to idle FTP clients. • Server side. The timeout value for data connections to idle FTP servers.

Step 5 Submit and commit your changes.

Related topics

- [Overview of FTP Proxy Services, page 5-14.](#)
- To configure proxy settings that apply to FTP over HTTP connections, see [Configuring Web Proxy Settings, page 5-3.](#)

SOCKS Proxy Services

- [Overview of SOCKS Proxy Services, page 5-16](#)
- [Enabling Processing of SOCKS Traffic, page 5-16](#)
- [Configuring the SOCKS Proxy, page 5-17](#)
- [Creating SOCKS Policies, page 5-17](#)

Overview of SOCKS Proxy Services

The Web Security appliance includes a SOCKS proxy to process SOCKS traffic. SOCKS policies are the equivalent of access policies and control SOCKS traffic. Similar to access policies, you can make use of Identities to specify which transactions are governed by which SOCKS policy. Once SOCKS policies are applied to transactions, Routing policies can then govern routing of the traffic.

Enabling Processing of SOCKS Traffic

Before you Begin

- Enable the Web Proxy.

Step 1 Choose **Security Services > SOCKS Proxy**.

Step 2 Click **Edit Settings**.



- Step 3** Select **Enable SOCKS Proxy**.
- Step 4** **Submit** and **Commit Changes**.

Configuring the SOCKS Proxy

- Step 1** Choose **Security Services > SOCKS Proxy**.
- Step 2** Click **Edit Settings**.
- Step 3** Select **Enable SOCKS Proxy**.
- Step 4** Configure the basic and advanced SOCKS Proxy settings.

Property	Description
SOCKS Proxy	Enabled.
SOCKS Control Ports	Ports that accept SOCKS requests. Default is 1080.
UDP Request Ports	UDP ports on which the SOCKS server should listen. Default is 16000-16100.
Proxy Negotiation Timeout	Time to wait (in seconds) to send or receive data from a SOCKS client in the negotiation phase. Default is 60.
UDP Tunnel Timeout	Time to wait (in seconds) for data from a UDP client or server before closing the UDP tunnel. Default is 60.

Creating SOCKS Policies

- Step 1** Choose **Web Security Manager > SOCKS Policies**.
- Step 2** Click **Add Policy**.
- Step 3** Assign a name in the **Policy Name** field.
-  **Note** Each policy group name must be unique and only contain alphanumeric characters or the space character.
- Step 4** (Optional) Add a description.
- Step 5** In the **Insert Above Policy** field, choose where in the SOCKS policies table to insert this SOCKS policy.
-  **Note** When configuring multiple SOCKS policies, determine a logical order for each policy. Order your policies to ensure that correct matching occurs.
- Step 6** In the **Identities and Users** section, choose one or more Identities to apply to this policy group.

Step 7 (Optional) Expand the Advanced section to define additional membership requirements.

Advanced Option	Description
Proxy Ports	<p>The port configured in the browser.</p> <p>(Optional) Define policy group membership by the proxy port used to access the Web Proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas.</p> <p>You might want to define policy group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port.</p> <p>Note If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the SOCKS policy group level.</p>
Subnets	<p>(Optional) Define policy group membership by subnet or other addresses.</p> <p>You can choose to use the addresses that may be defined with the associated Identity, or you can enter specific addresses here.</p> <p>Note If the Identity associated with this policy group defines its membership by addresses, then in this policy group you must enter addresses that are a subset of the Identity's addresses. Adding addresses in the policy group further narrows down the list of transactions that match this policy group.</p>
Time Range	<p>(Optional) Define policy group membership by time range:</p> <ol style="list-style-type: none"> 1. Select a time range from the Time Range field. 2. Specify whether this policy group should apply to the times inside or outside the selected time range.

Step 8 **Submit and Commit Changes.**

Related Topics

- (Optional) Add an Identity for use with SOCKS Policies.
- Add one or more SOCKS Policies to manage SOCKS traffic.

Troubleshooting Intercepting Requests

- [URL Categories Do Not Block Some FTP Sites, page A-4](#)
- [Large FTP Transfers Disconnect, page A-4](#)
- [Zero Byte File Appears On FTP Servers After File Upload, page A-4](#)
- [Unable to Route FTP Requests Via an Upstream Proxy, page A-13](#)
- [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, page A-9](#)
- [User Matches Global Policy for HTTPS and FTP over HTTP Requests, page A-9](#)



CHAPTER 6

Acquire End-User Credentials

- [Overview of Acquire End-User Credentials, page 6-1](#)
- [Authentication Best Practices, page 6-2](#)
- [Authentication Realms, page 6-3](#)
- [Failed Authentication, page 6-19](#)
- [Credentials, page 6-24](#)
- [Troubleshooting Authentication, page 6-25](#)

Overview of Acquire End-User Credentials

Server Type/Realm	Authentication Scheme	Supported Network Protocol	Notes
Active Directory	Kerberos NTLMSSP Basic	HTTP, HTTPS Native FTP, FTP over HTTP SOCKS (Basic authentication)	Kerberos is only supported in Standard mode. It is not supported in Cloud Connector mode.
LDAP	Basic	HTTP, HTTPS Native FTP, FTP over HTTP SOCKS	—

Authentication Task Overview

Step	Task	Links to Related Topics and Procedures
1.	Create an authentication realm.	<ul style="list-style-type: none"> • Creating an Active Directory Authentication Realm, page 6-6 • Creating an LDAP Authentication Realm, page 6-7
2.	Configure global authentication settings.	<ul style="list-style-type: none"> • Configuring Global Authentication Settings, page 6-12
3.	(Optional) Create and order additional authentication realms. Create at least one authentication realm for each authentication protocol and scheme combination you plan to use.	<ul style="list-style-type: none"> • Creating Authentication Sequences, page 6-18
4.	(Optional) Configure credential encryption.	<ul style="list-style-type: none"> • Configuring Credential Encryption, page 6-24
5.	Create identities to classify users and client software based on authentication requirements.	<ul style="list-style-type: none"> • Classifying Users and Client Software, page 7-3
6.	Create policies to manage web requests from the users and user groups for which you created identities.	<ul style="list-style-type: none"> • Managing Web Requests Through Policies Best Practices, page 10-2

Authentication Best Practices

- Create as few Active Directory realms as is practical. Multiple Active Directory realms require additional memory usage for authentication.
- If using NTLMSSP, authenticate users using either the Web Security appliance or the upstream proxy server, but not both. (Recommend Web Security appliance)
- If using Kerberos, authenticate using the Web Security appliance.
- For optimal performance, authenticate clients on the same subnet using a single realm.

Credentials

Authentication credentials are obtained from users by either prompting them to enter their credentials through their browsers, or another client application, or by obtaining the credentials transparently from another source.

- [Configuring Single-Sign-on, page 6-2](#)
- [Tracking Credentials for Reuse During a Session, page 6-3](#)
- [Authentication and Authorization Failures, page 6-3](#)

Configuring Single-Sign-on

Obtaining credentials transparently facilitates a single-sign-on environment. Transparent user identification is an authentication realm setting.

Tracking Credentials for Reuse During a Session

Using authentication surrogates, after a user authenticates once during a session, you can track credentials for reuse throughout that session rather than having the user authenticate for each new request. Authentication surrogates may be based on the IP address of the user's workstation or on a cookie that is assigned to the session.

Authentication and Authorization Failures

If authentication fails for accepted reasons, such as incompatible client applications, you can grant guest access.

If authentication succeeds but authorization fails, it is possible to allow re-authentication using a different set of credentials that may be authorized to access the requested resource.

Related Topics

- [Granting Guest Access After Failed Authentication, page 6-20](#)
- [Allowing Re-Authentication with Different Credentials, page 6-22](#)

Authentication Realms

- [About Authentication Realms, page 6-3](#)
- [Creating an Active Directory Realm for Kerberos Authentication Scheme, page 6-3](#)
- [Creating an Active Directory Authentication Realm, page 6-6](#)
- [Creating an LDAP Authentication Realm, page 6-7](#)
- [About Deleting Authentication Realms, page 6-11](#)
- [Configuring Global Authentication Settings, page 6-12](#)

About Authentication Realms

Authentication realms define the details required to contact the authentication servers and specify which authentication scheme to use when communicating with clients. AsyncOS supports multiple authentication realms. Realms can also be grouped into authentication sequences that allow users with different authentication requirements to be managed through the same policies.

Related Topics

- [Authentication Sequences, page 6-17](#)

Creating an Active Directory Realm for Kerberos Authentication Scheme

Before You Begin

- Ensure the appliance is configured in Standard mode (not Cloud Connector Mode).
- Prepare the Active Directory Server.

- Install Active Directory on one of these servers: Windows server 2003, 2008, 2008R2 or 2012.
 - Create a user on the Active Directory server that is a member of the domain administrators.
 - Join your client to the domain. Supported clients are Windows XP, Windows 7 and Mac OS 10.5+.
 - Use the kerbtray tool from the Windows Resource Kit to verify the Kerberos ticket on the client: <http://www.microsoft.com/en-us/download/details.aspx?id=17657> .
 - Ticket viewer application on Mac clients is available under main menu > KeyChain Access to view the Kerberos tickets.
- Ensure you have the rights and domain information needed to join the Web Security appliance to the Active Directory domain you wish to authenticate against.
 - Compare the current time on the Web Security appliance with the current time on the Active Directory server and verify that the difference is no greater than the time specified in the “Maximum tolerance for computer clock synchronization” option on the Active Directory server.
 - If the Web Security appliance is managed by a Security Management appliance, be prepared to ensure that same-named authentication realms on different Web Security appliances have identical properties defined on each appliance.
 - Be aware that once you commit the new realm, you cannot change a realm’s authentication protocol.

Step 1 In the Cisco Web Security Appliance web interface, choose **Network > Authentication**.

Step 2 Click **Add Realm**.

Step 3 Assign a unique name to the authentication realm using only alphanumeric and space characters.

Step 4 Select **Active Directory** in the Authentication Protocol field.

Step 5 Enter up to three fully-qualified domain names or IP addresses for the Active Directory server(s).

Example: `ntlm.example.com`.

An IP address is required only if the DNS servers configured on the appliance cannot resolve the Active Directory server hostname.

When multiple authentication servers are configured in the realm, the appliance attempts to authorize with up to three authentication servers before failing to authorize the transaction within this realm.

Step 6 Join the appliance to the domain:

- a. Configure the Active Directory Account:

Setting	Description
Active Directory Domain	The Active Directory server domain name. Also known as a DNS Domain or realm.

Setting	Description
NetBIOS domain name	If the network uses NetBIOS, provide the domain name. Tip If this option is not available use the <code>setntlmsecuritymode</code> CLI command to verify that the NTLM security mode is set to “domain”.
Computer Account	Specify a location within the Active Directory domain where AsyncOS will create an Active Directory computer account, also known as a “machine trust account”, to uniquely identify the computer on the domain. If the Active Directory environment automatically deletes computer objects at particular intervals, specify a location for the computer account that is in a container, protected from automatic deletion.

b. Click **Join Domain**.

Step 7 (Optional) Configure transparent user identification.

Setting	Description
Enable Transparent User Identification using Active Directory agent	Enter both the server name for the machine where the primary Active Directory agent is installed and the shared secret used to access it. (Optional) Enter the server name for the machine where a backup Active Directory agent is installed and its shared secret.

Step 8 Configure Network Security:

Setting	Description
Client Signing Required	Select this option if the Active Directory server is configured to require client signing. With this option selected, AsyncOS uses Transport Layer Security when communicating with the Active Directory server.

Step 9 (Optional) Click **Start Test**. This will test the settings you have entered, ensuring they are correct before real users use them to authenticate. For details on the testing performed, see [•Create additional NTLM realms to authenticate users in domains that are not trusted by existing NTLM realms., page 6-11.](#)

Step 10 Submit and commit your changes.

Tip

- Customize the access log to use the `%m` custom field parameter.

Next Step

- Create an Identity that uses the Kerberos authentication scheme. [Classifying Users and Client Software, page 7-3.](#)

Creating an Active Directory Authentication Realm

Before You Begin

- Ensure you have the rights and domain information needed to join the Web Security appliance to the Active Directory domain you wish to authenticate against.
- If you plan to use “domain” as the NTLM security mode, use only nested Active Directory groups. If Active Directory groups are not nested, use the default value, “ads”. See [setntlmsecuritymode](#) in the Command Line Interface appendix of this guide.
- Compare the current time on the Web Security appliance with the current time on the Active Directory server and verify that the difference is no greater than the time specified in the “Maximum tolerance for computer clock synchronization” option on the Active Directory server. If the Web Security appliance is managed by a Security Management appliance, be prepared to ensure that same-named authentication realms on different Web Security appliances have identical properties defined on each appliance. Be aware that once you commit the new realm, you cannot change a realm’s authentication protocol.

Step 1 Choose **Network > Authentication**.

Step 2 Click **Add Realm**.

Step 3 Assign a unique name to the authentication realm using only alphanumeric and space characters.

Step 4 Select **Active Directory** in the Authentication Protocol and Scheme(s) field.

Step 5 Enter up to three fully-qualified domain names or IP addresses for the Active Directory server(s).

Example: `active.example.com`.

An IP address is required only if the DNS servers configured on the appliance cannot resolve the Active Directory server hostname.

When multiple authentication servers are configured in the realm, the appliance attempts to authorize with up to three authentication servers before failing to authorize the transaction within this realm.

Step 6 Join the appliance to the domain:

- Configure the Active Directory Account:

Setting	Description
Active Directory Domain	The Active Directory server domain name. Also known as a DNS Domain or realm.
NetBIOS domain name	If the network uses NetBIOS, provide the domain name. Tip If this option is not available use the <code>setntlmsecuritymode</code> CLI command to verify that the NTLM security mode is set to “domain”.
Computer Account	Specify a location within the Active Directory domain where AsyncOS will create an Active Directory computer account, also known as a “machine trust account”, to uniquely identify the computer on the domain. If the Active Directory environment automatically deletes computer objects at particular intervals, specify a location for the computer account that is in a container, protected from automatic deletion.

- Click **Join Domain**.

- c. Enter the sAMAccountName user name and password for an existing Active Directory user that has rights to create computer accounts in the domain.

Example: “jazzdoe” Do not use: “DOMAIN\jazzdoe” or “jazzdoe@domain”

This information is used once to establish the computer account and is not saved.

- d. Click **Create Account**.

Step 7 (Optional) Configure transparent authentication.

Setting	Description
Enable Transparent User Identification using Active Directory agent	Enter both the server name for the machine where the primary Active Directory agent is installed and the shared secret used to access it. (Optional) Enter the server name for the machine where a backup Active Directory agent is installed and its shared secret.

Step 8 Configure Network Security:

Setting	Description
Client Signing Required	Select this option if the Active Directory server is configured to require client signing. With this option selected, AsyncOS uses Transport Layer Security when communicating with the Active Directory server.

Step 9 (Optional) Click **Start Test**. This will test the settings you have entered, ensuring they are correct before real users use them to authenticate.

Step 10 Submit and commit your changes.

Creating an LDAP Authentication Realm

Before You Begin

- Obtain the following information about LDAP in your organization:
 - LDAP version
 - Server addresses
 - LDAP ports
- If the Web Security appliance is managed by a Security Management appliance, ensure that same-named authentication realms on different Web Security appliances have identical properties defined on each appliance.

Step 1 Choose **Network > Authentication**.

Step 2 Click **Add Realm**.

Step 3 Assign a unique name to the authentication realm using only alphanumeric and space characters.

Step 4 Select **LDAP** in the Authentication Protocol and Scheme(s) field.

Step 5 Enter the LDAP authentication settings:

Setting	Description
LDAP Version	<p>Choose the version of LDAP, and choose whether or not to use Secure LDAP.</p> <p>The appliance supports LDAP versions 2 and 3. Secure LDAP requires LDAP version 3.</p> <p>Choose whether or not this LDAP server supports Novell eDirectory to use with transparent user identification.</p>
LDAP Server	<p>Enter the LDAP server IP address or hostname and its port number. You can specify up to three servers.</p> <p>The hostname must be a fully-qualified domain name. For example, <code>ldap.example.com</code>. An IP address is required only if the DNS servers configured on the appliance cannot resolve the LDAP server hostname.</p> <p>The default port number for Standard LDAP is 389. The default number for Secure LDAP is 636.</p> <p>If the LDAP server is an Active Directory server, enter the hostname or IP address and the port of the domain controller here. Whenever possible, enter the name of the Global Catalog Server and use port 3268. However, you might want to use a local domain controller when the global catalog server is physically far away and you know you only need to authenticate users on the local domain controller.</p> <p>Note: When you configure multiple authentication servers in the realm, the appliance attempts to authorize with up to three authentication servers before failing to authenticate the transaction within that realm.</p>
LDAP Persistent Connections (under the Advanced section)	<p>Choose one of the following values:</p> <ul style="list-style-type: none"> • Use persistent connections (unlimited). Use existing connections. If no connections are available a new connection is opened. • Use persistent connections. Use existing connections to service the number of requests specified. When the maximum is reached, establish a new connection to the LDAP server. • Do not use persistent connections. Always create a new connection to the LDAP server.

Setting	Description
User Authentication	<p>Enter values for the following fields:</p> <p>Base Distinguished Name (Base DN)</p> <p>The LDAP database is a tree-type directory structure and the appliance uses the Base DN to navigate to the correct location in the LDAP directory tree to begin a search. A valid Base DN filter string is composed of one or more components of the form <code>object-value</code>. For example <code>dc=companyname, dc=com</code>.</p> <p>User Name Attribute</p> <p>Choose one of the following values:</p> <ul style="list-style-type: none"> • uid, cn, and sAMAccountName. Unique identifiers in the LDAP directory that specify a username. • custom. A custom identifier such as <code>UserAccount</code>. <p>User Filter Query</p> <p>The User Filter Query is an LDAP search filter that locates the users Base DN. This is required if the user directory is in a hierarchy below the Base DN, or if the login name is not included in the user-specific component of that users Base DN.</p> <p>Choose one of the following values:</p> <ul style="list-style-type: none"> • none. Filters any user. • custom. Filters a particular group of users.
Query Credentials	<p>Choose whether or not the authentication server accepts anonymous queries.</p> <p>If the authentication server does accept anonymous queries, choose Server Accepts Anonymous Queries.</p> <p>If the authentication server does not accept anonymous queries, choose Use Bind DN and then enter the following information:</p> <ul style="list-style-type: none"> • Bind DN. The user on the external LDAP server permitted to search the LDAP directory. Typically, the bind DN should be permitted to search the entire directory. • Password. The password associated with the user you enter in the Bind DN field. <p>The following text lists some example users for the Bind DN field:</p> <pre>cn=administrator,cn=Users,dc=domain,dc=com sAMAccountName=jdoe,cn=Users,dc=domain,dc=com.</pre> <p>If the LDAP server is an Active Directory server, you may also enter the Bind DN username as "DOMAIN\username."</p>

Step 6 (Optional) Enable Group Authorization via group object or user object and complete the settings for the chosen option accordingly:

Group Object Setting	Description
Group Membership Attribute Within Group Object	<p>Choose the LDAP attribute which lists all users that belong to this group.</p> <p>Choose one of the following values:</p> <ul style="list-style-type: none"> • member and uniquemember. Unique identifiers in the LDAP directory that specify group members. • custom. A custom identifier such as <code>UserInGroup</code>.
Attribute that Contains the Group Name	<p>Choose the LDAP attribute which specifies the group name that can be used in the policy group configuration.</p> <p>Choose one of the following values:</p> <ul style="list-style-type: none"> • cn. A unique identifier in the LDAP directory that specifies the name of a group. • custom. A custom identifier such as <code>FinanceGroup</code>.
Query String to Determine if Object is a Group	<p>Choose an LDAP search filter that determines if an LDAP object represents a user group.</p> <p>Choose one of the following values:</p> <ul style="list-style-type: none"> • objectclass=groupofnames • objectclass=groupofuniquenames • objectclass=group • custom. A custom filter such as <code>objectclass=person</code>. <p>Note: The query defines the set of authentication groups which can be used in policy groups.</p>

User Object Setting	Description
Group Membership Attribute Within User Object	<p>Choose the attribute which list all the groups that this user belongs to.</p> <p>Choose one of the following values:</p> <ul style="list-style-type: none"> • memberOf. Unique identifiers in the LDAP directory that specify user members. • custom. A custom identifier such as <code>UserInGroup</code>.
Group Membership Attribute is a DN	<p>Specify whether the group membership attribute is a distinguished name (DN) which refers to an LDAP object. For Active Directory servers, enable this option.</p> <p>When this is enabled, you must configure the subsequent settings.</p>

User Object Setting	Description
Attribute that Contains the Group Name	<p>When the group membership attribute is a DN, this specifies the attribute that can be used as group name in policy group configurations.</p> <p>Choose one of the following values:</p> <ul style="list-style-type: none"> • cn. A unique identifier in the LDAP directory that specifies the name of a group. • custom. A custom identifier such as <code>FinanceGroup</code>.
Query String to Determine if Object is a Group	<p>Choose an LDAP search filter that determines if an LDAP object represents a user group.</p> <p>Choose one of the following values:</p> <ul style="list-style-type: none"> • objectclass=groupofnames • objectclass=groupofuniquenames • objectclass=group • custom. A custom filter such as <code>objectclass=person</code>. <p>Note: The query defines the set of authentication groups which can be used in Web Security Manager policies.</p>

Step 7 (Optional) Click **Start Test**. This will test the settings you have entered, ensuring they are correct before real users use them to authenticate. For details on the testing performed, see [•Create additional NTLM realms to authenticate users in domains that are not trusted by existing NTLM realms.](#), page 6-11.



Note Once you submit and commit your changes, you cannot later change a realm's authentication protocol.

Step 8 Submit and commit your changes.

Using Multiple NTLM Realms and Domains

The following rules apply in regard to using multiple NTLM realms and domains:

- You can create up to 10 NTLM authentication realms.
- The client IP addresses in one NTLM realm must not overlap with the client IP addresses in another NTLM realm.
- Each NTLM realm can join one Active Directory domain only but can authenticate users from any domains trusted by that domain. This trust applies to other domains in the same forest by default and to domains outside the forest to which at least a one way trust exists.
- Create additional NTLM realms to authenticate users in domains that are not trusted by existing NTLM realms.

About Deleting Authentication Realms

Deleting an authentication realm disables associated identities, which in turn removes those identities from associated policies.

Deleting an authentication realm removes it from sequences.

Configuring Global Authentication Settings

Configure Global Authentication Settings to apply settings to all authentication realms, independent of their authentication protocols.

The Web Proxy deployment mode affects which global authentication settings you can configure. More settings are available when it is deployed in transparent mode than in explicit forward mode.

Before You Begin

- Be familiar with the following concepts:
 - [Failed Authentication, page 6-19](#)
 - [Failed Authorization: Allowing Re-Authentication with Different Credentials, page 6-22](#)

Step 1 Choose **Network > Authentication**

Step 2 Click **Edit Global Settings**.

Step 3 Edit the settings in the Global Authentication Settings section:.

Setting	Description
Action if Authentication Service Unavailable	Choose one of the following values: <ul style="list-style-type: none"> • Permit traffic to proceed without authentication. Processing continues as if the user was authenticated. • Block all traffic if user authentication fails. Processing is discontinued and all traffic is blocked.
Failed Authentication Handling	When you grant users guest access in an Identity policy, this setting determines how the Web Proxy identifies and logs the user as a guest in the access logs. For more information on granting users guest access, see Granting Guest Access After Failed Authentication, page 6-20 .

Setting	Description
Re-authentication (Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction)	<p>This setting allows users to authenticate again if the user is blocked from a website due to a restrictive URL filtering policy or due to being restricted from logging into another IP address.</p> <p>The user sees a block page that includes a link that allows them to enter new authentication credentials. If the user enters credentials that allow greater access, the requested page appears in the browser.</p> <p>Note: This setting only applies to authenticated users who are blocked due to restrictive URL filtering policies or User Session Restrictions. It does not apply to blocked transactions by subnet with no authentication.</p> <p>For more information, see Failed Authorization: Allowing Re-Authentication with Different Credentials, page 6-22.</p>
Basic Authentication Token TTL	<p>Controls the length of time that user credentials are stored in the cache before revalidating them with the authentication server. This includes the username and password and the directory groups associated with the user.</p> <p>The default value is the recommended setting. When the Surrogate Timeout setting is configured and is greater than the Basic Authentication Token TTL, then the Surrogate Timeout value takes precedence and the Web Proxy contacts the authentication server after surrogate timeout expires.</p>

The remaining authentication settings you can configure depends on how the Web Proxy is deployed, in transparent or explicit forward mode.

Step 4 If the Web Proxy is deployed in transparent mode, edit the settings as follows:

Setting	Description
Credential Encryption	<p>This setting specifies whether or not the client sends the login credentials to the Web Proxy through an encrypted HTTPS connection.</p> <p>This setting applies to both Basic and NTLMSSP authentication schemes, but it is particularly useful for Basic authentication scheme because user credentials are sent as plain text.</p> <p>For more information, see Failed Authentication, page 6-19.</p>
HTTPS Redirect Port	<p>Specify a TCP port to use for redirecting requests for authenticating users over an HTTPS connection.</p> <p>This specifies through which port the client will open a connection to the Web Proxy using HTTPS. This occurs when credential encryption is enabled or when using Access Control and users are prompted to authenticate.</p>

Setting	Description
Redirect Hostname	<p>Enter the short hostname of the network interface on which the Web Proxy listens for incoming connections.</p> <p>When you configure authentication on an appliance deployed in transparent mode, the Web Proxy uses this hostname in the redirection URL sent to clients for authenticating users.</p> <p>You can enter either the following values:</p> <ul style="list-style-type: none"> Single word hostname. You can enter the single word hostname that is DNS resolvable by the client and the Web Security appliance. This allows clients to achieve true single sign-on with Internet Explorer without additional browser side setup. <p>Be sure to enter the single word hostname that is DNS resolvable by the client and the Web Security appliance.</p> <p>For example, if your clients are in domain <code>mycompany.com</code> and the interface on which the Web Proxy is listening has a full hostname of <code>proxy.mycompany.com</code>, then you should enter <code>proxy</code> in this field. Clients perform a lookup on <code>proxy</code> and they should be able to resolve <code>proxy.mycompany.com</code>.</p> Fully qualified domain name (FQDN). You can also enter the FQDN or IP address in this field. However, if you do that and want true single sign-on for Internet Explorer and Firefox browsers, you must ensure that the FQDN or IP address is added to the client's Trusted Sites list in the client browsers. <p>The default value is the FQDN of the M1 or P1 interface, depending on which interface is used for proxy traffic.</p>
Credential Cache Options: Surrogate Timeout	<p>This setting specifies how long the Web Proxy waits before asking the client for authentication credentials again. Until the Web Proxy asks for credentials again, it uses the value stored in the surrogate (IP address or cookie).</p> <p>It is common for user agents, such as browsers, to cache the authentication credentials so the user will not be prompted to enter credentials each time.</p>
Credential Cache Options: Client IP Idle Timeout	<p>When IP address is used as the authentication surrogate, this setting specifies how long the Web Proxy waits before asking the client for authentication credentials again when the client has been idle.</p> <p>When this value is greater than the Surrogate Timeout value, this setting has no effect and clients are prompted for authentication after the Surrogate Timeout is reached.</p> <p>You might want to use this setting to reduce the vulnerability of users who leave their computers.</p>
Credential Cache Options: Cache Size	<p>Specifies the number of entries that are stored in the authentication cache. Set this value to safely accommodate the number of users that are actually using this device. The default value is the recommended setting.</p>

Setting	Description
User Session Restrictions	<p>This setting specifies whether or not authenticated users are allowed to access the Internet from multiple IP addresses simultaneously.</p> <p>You might want to restrict access to one machine to prevent users from sharing their authentication credentials with non-authorized users. When a user is prevented from logging in at a different machine, an end-user notification page appears. You can choose whether or not users can click a button to login as a different username using the Re-authentication setting on this page.</p> <p>When you enable this setting, enter the restriction timeout value, which determines how long users must wait before being able to log into a machine with a different IP address. The restriction timeout value must be greater than the surrogate timeout value.</p> <p>You can remove a specific user or all users from the authentication cache using the <code>authcache</code> CLI command.</p>
Advanced	<p>When using Credential Encryption or Access Control, you can choose whether the appliance uses the digital certificate and key shipped with the appliance (the Cisco Web Security Appliance Demo Certificate) or a digital certificate and key you upload here.</p>

Step 5 If the Web Proxy is deployed in explicit forward mode, edit the settings as follows:

Setting	Description
Credential Encryption	<p>This setting specifies whether or not the client sends the login credentials to the Web Proxy through an encrypted HTTPS connection. To enable credential encryption, choose “HTTPS Redirect (Secure)”. When you enable credential encryption, additional fields appear to configure how to redirect clients to the Web Proxy for authentication.</p> <p>This setting applies to both Basic and NTLMSSP authentication schemes, but it is particularly useful for Basic authentication scheme because user credentials are sent as plain text.</p> <p>For more information, see Failed Authentication, page 6-19.</p>
HTTPS Redirect Port	<p>Specify a TCP port to use for redirecting requests for authenticating users over an HTTPS connection.</p> <p>This specifies through which port the client will open a connection to the Web Proxy using HTTPS. This occurs when credential encryption is enabled or when using Access Control and users are prompted to authenticate.</p>

Setting	Description
Redirect Hostname	<p>Enter the short hostname of the network interface on which the Web Proxy listens for incoming connections.</p> <p>When you enable Authentication Mode above, the Web Proxy uses this hostname in the redirection URL sent to clients for authenticating users.</p> <p>You can enter either the following values:</p> <ul style="list-style-type: none"> Single word hostname. You can enter the single word hostname that is DNS resolvable by the client and the Web Security appliance. This allows clients to achieve true single sign-on with Internet Explorer without additional browser side setup. <p>Be sure to enter the single word hostname that is DNS resolvable by the client and the Web Security appliance.</p> <p>For example, if your clients are in domain <code>mycompany.com</code> and the interface on which the Web Proxy is listening has a full hostname of <code>proxy.mycompany.com</code>, then you should enter <code>proxy</code> in this field. Clients perform a lookup on <code>proxy</code> and they should be able to resolve <code>proxy.mycompany.com</code>.</p> Fully qualified domain name (FQDN). You can also enter the FQDN or IP address in this field. However, if you do that and want true single sign-on for Internet Explorer and Firefox browsers, you must ensure that the FQDN or IP address is added to the client's Trusted Sites list in the client browsers. <p>The default value is the FQDN of the M1 or P1 interface, depending on which interface is used for proxy traffic.</p>
Credential Cache Options: Surrogate Timeout	<p>This setting specifies how long the Web Proxy waits before asking the client for authentication credentials again. Until the Web Proxy asks for credentials again, it uses the value stored in the surrogate (IP address or cookie).</p> <p>Note that it is common for user agents, such as browsers, to cache the authentication credentials so the user will not be prompted to enter credentials each time.</p>
Credential Cache Options: Client IP Idle Timeout	<p>When IP address is used as the authentication surrogate, this setting specifies how long the Web Proxy waits before asking the client for authentication credentials again when the client has been idle.</p> <p>When this value is greater than the Surrogate Timeout value, this setting has no effect and clients are prompted for authentication after the Surrogate Timeout is reached.</p> <p>You might want to use this setting to reduce the vulnerability of users who leave their computers.</p>
Credential Cache Options: Cache Size	<p>Specifies the number of entries that are stored in the authentication cache. Set this value to safely accommodate the number of users that are actually using this device. The default value is the recommended setting.</p>

Setting	Description
User Session Restrictions	<p>This setting specifies whether or not authenticated users are allowed to access the Internet from multiple IP addresses simultaneously.</p> <p>You might want to restrict access to one machine to prevent users from sharing their authentication credentials with non-authorized users. When a user is prevented from logging at a different machine, an end-user notification page appears. You can choose whether or not users can click a button to login as a different username using the Re-authentication setting on this page.</p> <p>When you enable this setting, enter the restriction timeout value, which determines how long users must wait before being able to log into a machine with a different IP address. The restriction timeout value must be greater than the surrogate timeout value.</p> <p>You can remove a specific user or all users from the authentication cache using the <code>authcache</code> CLI command.</p>
Advanced	<p>When using Credential Encryption or Access Control, you can choose whether the appliance uses the digital certificate and key shipped with the appliance (the Cisco Web Security Appliance Demo Certificate) or a digital certificate and key you upload here.</p> <p>To upload a digital certificate and key, click Browse and navigate to the necessary file on your local machine. Then click Upload Files after you select the files you want.</p>

Step 6 Submit and commit your changes.

Authentication Sequences

- [About Authentication Sequences, page 6-17](#)
- [Creating Authentication Sequences, page 6-18](#)
- [Editing And Reordering Authentication Sequences, page 6-18](#)
- [Editing And Reordering Authentication Sequences, page 6-18](#)

About Authentication Sequences

Use authentication sequences to allow single Identities to authenticate users via different authentication servers or protocols. Authentication sequences are also useful for providing backup options in case primary authentication options become unavailable.

Authentication sequences are collections of two or more authentication realms. The realms used can have different authentication servers and different authentication protocols. For more information on authentication realms, see [Authentication Realms, page 6-3](#).

After you create a second authentication realm, the appliance automatically displays a Realm Sequences section under Network > Authentication and includes a default authentication sequence named All Realms. The All Realms sequence automatically includes each realm you define. You can change the order of the realms within the All Realms sequence, but you cannot delete the All Realms sequence or remove any realms from it.

When multiple NTLM authentication realms are defined, the Web Security appliance uses the NTLMSSP authentication scheme with only one NTLM authentication realm per sequence. You can choose which NTLM authentication realm to use for NTLMSSP within each sequence, including the All Realms sequence. To use NTLMSSP with multiple NTLM realms, define a separate Identity for each realm.

Which authentication realms within a sequence get used during authentication depends on:

- The authentication scheme used. This is generally dictated by the type of credentials entered at the client.
- The order in which realms are listed within the sequence (for Basic realms only, as only one NTLMSSP realm is possible).



Tip

For optimal performance, authenticate clients on the same subnet using a single realm.

Creating Authentication Sequences

Before You Begin

- Create two or more authentication realms (see [Authentication Realms, page 6-3](#)).
- If the Web Security appliance is managed by a Security Management appliance, ensure that same-named authentication realms on different Web Security appliances have identical properties defined on each appliance. Be aware that AsyncOS will use the realms to process authentication sequentially, beginning with the first realm in the list.

-
- Step 1** Choose **Network > Authentication**
 - Step 2** Click **Add Sequence**.
 - Step 3** Enter a unique name for the sequence using alphanumeric and space characters.
 - Step 4** In the first row of the Realm Sequence for Basic Scheme area, choose the first authentication realm you want to include in the sequence.
 - Step 5** In the second row of the Realm Sequence for Basic Scheme area, choose the next realm you want to include in the sequence.
 - Step 6** (Optional) Click **Add Row** to include another realm that uses Basic credentials.
 - Step 7** If an NTLM realm is defined, choose an NTLM realm in the Realm for NTLMSSP Scheme field.
The Web Proxy uses this NTLM realm when the client sends NTLMSSP authentication credentials.
 - Step 8** Submit and commit your changes.
-

Editing And Reordering Authentication Sequences

-
- Step 1** Choose **Network > Authentication**.
 - Step 2** Click the name of the sequence you wish to edit or re-order.
 - Step 3** Choose a realm name from the Realms drop-down list on the row corresponding to the position number you want the realm to occupy in the sequence.



Note For the All Realms sequence, you can only change the order of its realms, you cannot change the realms themselves. To change the order of realms in the All Realms sequence, click the arrows in the Order column to reposition the corresponding realms.

- Step 4** Repeat Step 3 until all realms are listed and ordered as required, ensuring that each realm name appears in one row only.
- Step 5** Submit and commit your changes.

Deleting Authentication Sequences

Before You Begin

- Be aware that deleting an authentication sequence also disables associated identities, which in turn removes those identities from associated policies.

- Step 1** Choose **Network > Authentication**.
- Step 2** Click the trash can icon for the sequence name.
- Step 3** Click **Delete** to confirm that you want to delete the sequence.
- Step 4** Commit your changes.

Failed Authentication

- [About Failed Authentication, page 6-19](#)
- [Bypassing Authentication, page 6-20](#)

About Failed Authentication

Users may be blocked from the web due to authentication failure for the following reason:

- **Client limitations.** Some client applications may not properly support authentication. You can bypass authentication for these clients by configuring Identities that do not require authorization and basing their criteria on the clients (and, optionally, on the URLs they need to access).
- **Authentication service is unavailable.** An authentication service might be unavailable due to network or server issues. You can choose to allow unauthenticated traffic in this circumstance.
- **Invalid credentials.** Some users may be unable to supply valid credentials for proper authentication (for example, visitors or users awaiting credentials). You can choose to grant these users limited access to the web.

Related Topics

- [Bypassing Authentication, page 6-20](#)
- [Permitting Unauthenticated Traffic While Authentication Service is Unavailable, page 6-20](#)

- [Granting Guest Access After Failed Authentication, page 6-20](#)

Bypassing Authentication

Step	More Information
1. Create a custom URL category that contains the affected websites by configuring the Advanced properties.	
2. Create an identity with these characteristics: <ul style="list-style-type: none"> – Placed above all identities that require authentication. – Includes the custom URL category. – Includes affected client applications. – Does not require authentication 	Classifying Users and Client Software, page 7-3
3. Create a policy for the identity.	Creating a Policy, page 10-5

Related Topics

- [Bypassing the Web Proxy](#)

Permitting Unauthenticated Traffic While Authentication Service is Unavailable



Note

This configuration applies only when an authentication service is unavailable. It will not bypass authentication permanently. For alternative options, see [About Failed Authentication, page 6-19](#)

-
- Step 1** Choose **Network > Authentication**.
 - Step 2** Click **Edit Global Settings**.
 - Step 3** Click the **Permit Traffic To Proceed Without Authentication** in the Action If Authentication Service Unavailable field.
 - Step 4** Submit and commit your changes.
-

Granting Guest Access After Failed Authentication

Granting guest access requires that the following procedures are completed:

1. [Define an Identity that Supports Guest Access, page 6-21](#)
2. [Use an Identity that Supports Guest Access in a Policy, page 6-21](#)
3. (Optional) [Configure How Guest User Details are Logged, page 6-21](#)

**Note**

If an Identity allows guest access and there is no user-defined policy that uses that Identity, users who fail authentication match the global policy of the applicable policy type. For example, if MyIdentity allows guest access and there is no user-defined Access Policy that uses MyIdentity, users who fail authentication match the global Access Policy. If you do not want guest users to match a global policy, create a policy above the global policy that applies to guest users and blocks all access.

Define an Identity that Supports Guest Access

-
- Step 1** Choose **Web Security Manager > Identities**.
 - Step 2** Click **Add Identity** to add a new identity, or click the name of an existing identity that you wish to use.
 - Step 3** Check the **Support Guest Privileges** check box.
 - Step 4** Submit and commit your changes.
-

Use an Identity that Supports Guest Access in a Policy

-
- Step 1** Choose a policy type from the Web Security Manager menu.
 - Step 2** Click a policy name in the policies table.
 - Step 3** Choose **Select One Or More Identities** from the Identities And Users drop-down list (if not already chosen).
 - Step 4** Choose an identity that supports guest access from the drop-down list in the Identity column.
 - Step 5** Click the **Guests (Users Failing Authentication)** radio button.

**Note**

If this option is not available it means the identity you chose is not configured to support guest access. Return to step 4 and choose another, or see [Define an Identity that Supports Guest Access, page 6-21](#) to define a new one.

-
- Step 6** Submit and commit your changes.
-

Configure How Guest User Details are Logged

-
- Step 1** Choose **Network > Authentication**.
 - Step 2** Click **Edit Global Settings**.
 - Step 3** Click a Log Guest User By radio button, described below, in the Failed Authentication Handling field.

Radio button	Description
IP Address	The IP address of the guest user's client will be logged in the access logs.
User Name As Entered By End-User	The user name that originally failed authentication will be logged in the access logs.

Step 4 Submit and commit your changes.

Failed Authorization: Allowing Re-Authentication with Different Credentials

- [About Allowing Re-Authentication with Different Credentials, page 6-22](#)
- [Allowing Re-Authentication with Different Credentials, page 6-22](#)

About Allowing Re-Authentication with Different Credentials

Use re-authentication to allow users the opportunity to authenticate again, using different credentials, if the credentials they previously used have failed authorization. A user may authenticate successfully but still be prevented from accessing a web resource if not authorized to do so. This is because authentication merely identifies users for the purpose of passing their verified credentials on to policies, but it is the policies that authorize those users (or not) to access resources.

A user must have authenticated successfully to be allowed to re-authenticate.

To use the re-authentication feature with user defined end-user notification pages, the CGI script that parses the redirect URL must parse and use the Reauth_URL parameter.

Allowing Re-Authentication with Different Credentials

- Step 1** Choose **Network > Authentication**.
- Step 2** Click **Edit Global Settings**.
- Step 3** Check the **Re-Authentication Prompt If End User Blocked by URL Category Or User Session Restriction** check box.
- Step 4** Click **Submit**.
-

Tracking Identified Users



Note

When the appliance is configured to use cookie-based authentication surrogates, it does not get cookie information from clients for HTTPS and FTP over HTTP requests. Therefore, it cannot get the user name from the cookie.

Surrogate Types	Credential Encryption Disabled			Credential Encryption Enabled		
	HTTP	HTTPS & FTP over HTTP	Native FTP	HTTP	HTTPS & FTP over HTTP	Native FTP
No Surrogate	Yes	Yes	Yes	NA	NA	NA

Surrogate Types	Credential Encryption Disabled			Credential Encryption Enabled		
IP-based	Yes	Yes	Yes	Yes	Yes	Yes
Cookie-based	Yes	Yes***	Yes***	Yes	No/Yes**	Yes***

Surrogate Types	Credential Encryption Disabled			Credential Encryption Enabled		
	Protocol:	HTTP	HTTPS	Native FTP	HTTP	HTTPS
No Surrogate	NA	NA	NA	NA	NA	NA
IP-based	Yes	No/Yes*	No/Yes*	Yes	No/Yes*	No/Yes*
Cookie-based	Yes	No/Yes**	No/Yes**	Yes	No/Yes**	No/Yes**

* Works after the client makes a request to an HTTP site and is authenticated. Before this happens, the behavior depends on the transaction type:

- **Native FTP transactions.** Transactions bypass authentication.
- **HTTPS transactions.** Transactions are dropped. However, you can configure the HTTPS Proxy to decrypt the first HTTPS request for authentication purposes.

** When cookie-based authentication is used, the Web Proxy cannot authenticate the user for HTTPS, native FTP, and FTP over HTTP transactions. Due to this limitation, all HTTPS, native FTP, and FTP over HTTP requests bypass authentication, so authentication is not requested at all.

*** No surrogate is used in this case even though cookie-based surrogate is configured.

Tracking Re-Authenticated Users

With re-authentication, if a more privileged user authenticates and is authorized, the Web Proxy caches this user identity for different amounts of time depending on the authentication surrogates configured:

- **Session cookie.** The privileged user identity is used until the browser is closed or the session times out.
- **Persistent cookie.** The privileged user identity is used until the surrogate times out.
- **IP address.** The privileged user identity is used until the surrogate times out.
- **No surrogate.** By default, the Web Proxy requests authentication for every new connection, but when re-authentication is enabled, the Web Proxy requests authentication for every new request, so there is an increased load on the authentication server when using NTLMSSP. The increase in authentication activity may not be apparent to a user, however, because most browsers will cache the privileged user credentials and authenticate without prompting until the browser is closed. Also, when the Web Proxy is deployed in transparent mode, and the “Apply same surrogate settings to explicit forward requests” option is not enabled, no authentication surrogates are used for explicit forward requests and increased load will occur with re-authentication.



Note

If the Web Security appliance uses cookies for authentication surrogates, Cisco recommends enabling credential encryption.

Credentials

- [Credential Format, page 6-24](#)
- [Credential Encryption for Basic Authentication, page 6-24](#)

Credential Format

Authentication Scheme	Credential Format
NTLMSSP	MyDomain\jsmith
Basic	jsmith
	MyDomain\jsmith
	Note If the user does not enter the Windows domain, the Web Proxy prepends the default Windows domain.

Credential Encryption for Basic Authentication

About Credential Encryption for Basic Authentication

Enable credential encryption to transmit credentials over HTTPS in encrypted form. This increases security of the basic authentication process.

The Web Security appliance uses its own certificate and private key by default to create an HTTPS connection with the client for the purposes of secure authentication. Most browsers will warn users, however, that this certificate is not valid. To prevent users from seeing the invalid certificate message, you can upload a valid certificate and key pair that your organization uses.

Configuring Credential Encryption

Before You Begin:

- Configure the appliance to use IP surrogates.
- (Optional) Obtain a certificate and unencrypted private key. The certificate and key configured here are also used by Access Control.

-
- Step 1** Choose **Network > Authentication**.
 - Step 2** Click **Edit Global Settings**.
 - Step 3** Check the **Use Encrypted HTTPS Connection For Authentication** check box in the Credential Encryption field.
 - Step 4** (Optional) Edit the default port number (443) in the HTTPS Redirect Port field for client HTTP connections during authentication.
 - Step 5** (Optional) Upload a certificate and key:
 - a. Expand the Advanced section.
 - b. Click **Browse** in the Certificate field and find the certificate file you wish to upload.
 - c. Click **Browse** in the Key field and find the private key file you wish to upload.

d. Click **Upload Files**.

Step 6 Submit and commit your changes.

Related Topics

- [Obtaining Certificates, page 21-23.](#)

Troubleshooting Authentication

- [LDAP User Fails Authentication due to NTLMSSP, page A-2](#)
- [LDAP Authentication Fails due to LDAP Referral, page A-2](#)
- [Basic Authentication Fails, page A-2](#)
- [Users Erroneously Prompted for Credentials, page A-3](#)
- [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, page A-9](#)
- [Cannot Access URLs that Do Not Support Authentication, page A-12](#)
- [Client Requests Fail Upstream Proxy, page A-13](#)



Classify End-Users and Client Software

- [Overview of Classify Users and Client Software, page 7-1](#)
- [Classify Users and Client Software: Best Practices, page 7-2](#)
- [Identity Criteria, page 7-2](#)
- [Classifying Users and Client Software, page 7-3](#)
- [Identities and Authentication, page 7-7](#)
- [Troubleshooting Identities, page 7-8](#)

Overview of Classify Users and Client Software

Identities classify users and user agents for these purposes:

- Application of policies (except SaaS)
- Specification of identification and authentication requirements

AsyncOS assigns an identity to every transaction:

- Custom Identities — AsyncOS assigns a custom identity based on that identity's criteria.
- The Global Identity — AsyncOS assigns the global identity to transactions that do not meet the criteria for any custom identity. By default, the global identity does not require authentication.

AsyncOS processes identities sequentially, beginning with the first identity. The global identity is the last identity.

An identity can include only one criterion. Identities that include multiple criteria require that all the criteria are met.

One policy may call on multiple identities:

The screenshot shows the 'Identities and Users' configuration page. It features a table with four rows, each representing an identity. The 'Identity' column contains dropdown menus for 'IdentityPolicy2', 'IdentityPolicy1', 'IdentityPolicyForFTP', and 'IdentityPolicy4'. The 'Authorized Users and Groups' column shows the configuration for each identity, including radio buttons for 'All Authenticated Users', 'Selected Groups and Users', and 'Guests (users failing authentication)'. A 'Realms' dropdown is visible for the first two identities. A 'No authentication required' option is present for the third identity. A 'Trash' icon is in the rightmost column of each row.

Four arrows point from the following text to the corresponding rows in the table:

- This Identity allows guest access and applies to users who fail authentication. (Points to IdentityPolicy2)
- Authentication is not used for this Identity. (Points to IdentityPolicyForFTP)
- The specified user groups in this Identity are authorized for this policy. (Points to IdentityPolicy1)
- This Identity uses an authentication sequence and this policy applies to one realm in the sequence. (Points to IdentityPolicy4)

Classify Users and Client Software: Best Practices

- Create fewer, more general Identities that apply to all users or fewer, larger groups of users. Use policies, rather than identities, for more granular management.
- Create Identities with unique criteria.
- If deployed in transparent mode, create an Identity for sites that do not support authentication. See [Bypassing Authentication, page 6-20](#).

Identity Criteria

Option	Description
Subnet	The client subnet must match the list of subnets in a policy
Protocol	The protocol used in the transaction, either HTTP, HTTPS, SOCKS, or native FTP
Port	The proxy port of the request must be in the Identity's list of ports, if any listed. For explicit forward connections this is the port configured in the browser. For transparent connections this is the same as the destination port.

Option	Description
User Agent	The user agent (client software) making the request must be in the Identity's list of user agents, if any are listed. Some user agents cannot handle authentication, therefore creating an identity that does not require authentication is necessary.
URL Category	The URL category of the request URL must be in the Identity's list of URL categories, if any are listed.
Authentication requirements	If the Identity requires authentication, the client authentication credentials must match the Identity's authentication requirements.

Classifying Users and Client Software

Before you Begin

- Create authentication realms. See [Creating an Active Directory Authentication Realm, page 6-6](#) or [Creating an LDAP Authentication Realm, page 6-7](#).
- Be aware that when you commit a change to Identities, end-users must re-authenticate.
- (Optional) Create authentication sequences. See [Creating Authentication Sequences, page 6-18](#)
- (Optional) Enable Secure Mobility if the identity will include mobile users.
- (Optional) Understand authentication surrogates. See [Tracking Identified Users, page 6-22](#).

Step 1 Choose **Web Security Manager > Identities**.

Step 2 Click **Add Identity**.

Step 3 Assign a name that is unique to Identities.

Step 4 (Optional) Enter a description.

Step 5 In the **Insert Above** field drop-down list, choose where in the table to place the Identity.



Note Position Identities that do not require authentication above the first Identity that requires authentication.

Step 6 In the **Define Members by User Location** section, configure the Identity to apply to local users, remote users, or both local and remote users. The setting chosen here affects the available authentication settings for this Identity.

Step 7 In the **Define Members by Subnet** field, enter the addresses to which this Identity should apply. Enter IP addresses, CIDR blocks, and subnets.



Note If no address is entered in this field, the Identity applies to *all* IP addresses.

Step 8 In the **Define Members by Protocol** section, check to select the protocols to which this Identity should apply. Select all that apply:

Option	Description
HTTP/HTTPS	Applies to all requests that use HTTP or HTTPS as the underlying protocol, including FTP over HTTP and any other protocol tunneled using HTTP CONNECT.
Native FTP	Applies to native FTP requests only
SOCKS	Applies to SOCKS Policies only

Step 9 In the **Identification and Authentication** field, choose an Identity authentication requirement from the following options:


Option	Description	Method
No Authentication	The user is identified primarily by IP address	Go to Step 11
Identify Users Transparently through Cisco ASA Integration	The user is identified by the current IP address to user name mapping received from the Cisco adaptive security appliance (ASA). This option appears when Secure Mobility is enabled and integrates with a Cisco adaptive security appliance.	<ol style="list-style-type: none"> a. In the Select a Realm or Sequence field, choose a defined authentication realm or sequence. b. If you chose an NTLM authentication realm or sequence that contains an NTLM authentication realm, then go to Step 10 to choose the authentication scheme.

Option	Description	Method
Identify Users Transparently	<p>The user is identified by the current IP address to user name mapping. This option appears when at least one authentication realm is defined that supports transparent user identification.</p> <p>Note (For deployments with a Security Management appliance) When configuring Identities on a Security Management appliance, this option appears when a Web Security appliance with an authentication realm that supports transparent user identification has been added as a managed appliance.</p>	<p>a. In the Select a Realm or Sequence field, choose a defined authentication realm that supports transparent user identification;</p> <ul style="list-style-type: none"> – an LDAP authentication realm that supports Novell eDirectory – an NTLM authentication realm that is enabled for transparent user identification. – You can also choose a sequence that contains only realms that support transparent user identification. <p>b. Choose whether to grant users guest access, or force an authentication prompt to appear to end users when transparent user identification fails.</p> <p>c. To grant guest access to users who fail authentication due to invalid credentials, select the Support Guest privileges check box.</p>
Authenticate User	<p>The user is identified by the authentication credentials entered. This option appears when at least one authentication realm is defined</p>	<p>a. In the Select a Realm or Sequence field, choose a defined authentication realm or sequence.</p> <p>b. To grant guest access to users who fail authentication due to invalid credentials, select the Support Guest privileges check box.</p>

Step 10 If you chose an Active Directory authentication realm or sequence that contains an Active Directory authentication realm, then choose the authentication scheme in the Select a Scheme field.

Step 11 Choose the settings in the **Authentication Surrogate** section, when authentication is required (a protocol must first be defined). These settings specify the way that transactions will be associated with a user after the user has authenticated successfully.

Options vary depending on the Web Proxy deployment mode.

Surrogate Type	Description
IP Address	<p>The Web Proxy tracks an authenticated user at a particular IP address.</p> <p style="text-align: center;"> Tip</p> <p>For transparent user identification, choose IP Address.</p>
Persistent Cookie	<p>The Web Proxy tracks an authenticated user on a particular application by generating a persistent cookie for each user per application. Closing the application does not remove the cookie.</p>

Surrogate Type	Description
Session Cookie	The Web Proxy tracks an authenticated user on a particular application by generating a session cookie for each user per domain per application. (However, when a user provides different credentials for the same domain from the same application, the cookie is overwritten.) Closing the application removes the cookie.
No Surrogate	The Web Proxy does not use a surrogate to cache the credentials, and it tracks an authenticated user for every new TCP connection. When you choose this option, the web interface disables other settings that no longer apply. This option is available only in explicit forward mode and when you disable credential encryption on the Network > Authentication page.
Apply same surrogate settings to explicit forward requests	Select whether or not the surrogate used for transparent requests should also be used for explicit requests. Selecting this will enable credential encryption automatically. This option appears only when the Web Proxy is deployed in transparent mode.

**Note**

You can define a timeout value for the authentication surrogate for all requests using Global Authentication Settings.

Step 12 (Optional) Expand the **Advanced** section to define additional membership requirements.

Advanced Option	Description
Proxy Ports	The proxy port is used to access the Web Proxy by entering one or more port numbers in the Proxy Ports field. Separate multiple ports with commas. For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. Note Defining identities by port works best when the appliance is deployed in explicit forward mode or when clients explicitly forward requests to the appliance. Defining identities by port when client requests are transparently redirected to the appliance may result in some requests being denied.
URL Categories	Select the user defined or predefined URL categories. Membership for both is excluded by default, meaning the Web Proxy ignores all categories unless they are selected in the Add column. Note If you need to define membership by URL category, only define it in the Identity group when you need to exempt from authentication requests to that category.
User Agents	Defines the policy group membership by the user agent (applications such as Firefox or Chrome Web browsers) used in the client request. You can select some commonly defined browsers, or define your own using regular expressions. Choose whether this policy group should apply to the selected user agents or to any user agent that is not in the list of selected user agents.

Step 13 Submit and Commit Changes.**Related Topics**

- [Overview of Acquire End-User Credentials, page 6-1](#)
- [Managing Web Requests Through Policies Task Overview, page 10-2](#)

Enable/Disable an Identity

Before You Begin

- Be aware that disabling an identity removes it from associated policies.
- Be aware that reenabling an identity does not re-associate it with any policies.

-
- Step 1** Choose **Web Security Manager > Identities**.
- Step 2** Click a policy name in the policies table.
- Step 3** Check or uncheck Enable Identity in the Identity Settings field.
- Step 4** **Submit and Commit Changes**.
-

Identities and Authentication

[Figure 7-1 on page 7-8](#) shows how the Web Proxy evaluates a client request against the Identities when the Identity is configured to use:

- No authentication surrogates
- IP addresses as authentication surrogates
- Cookies as authentication surrogates with transparent requests
- Cookies as authentication surrogates with explicit requests and credential encryption is enabled

Figure 7-1 Transaction Request flow: Identities and Authentication - No Surrogates and IP-Based Surrogates

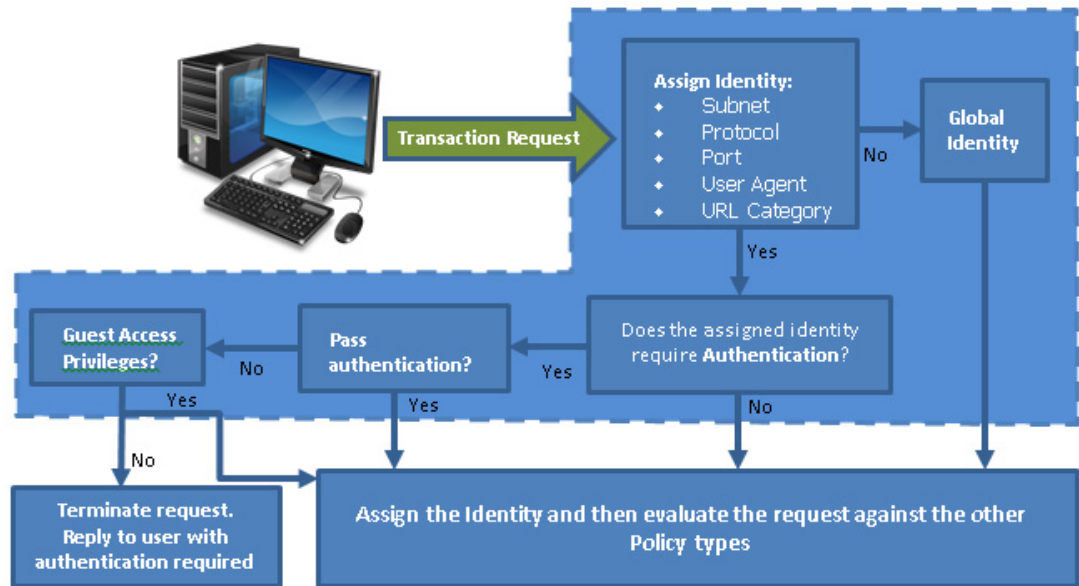
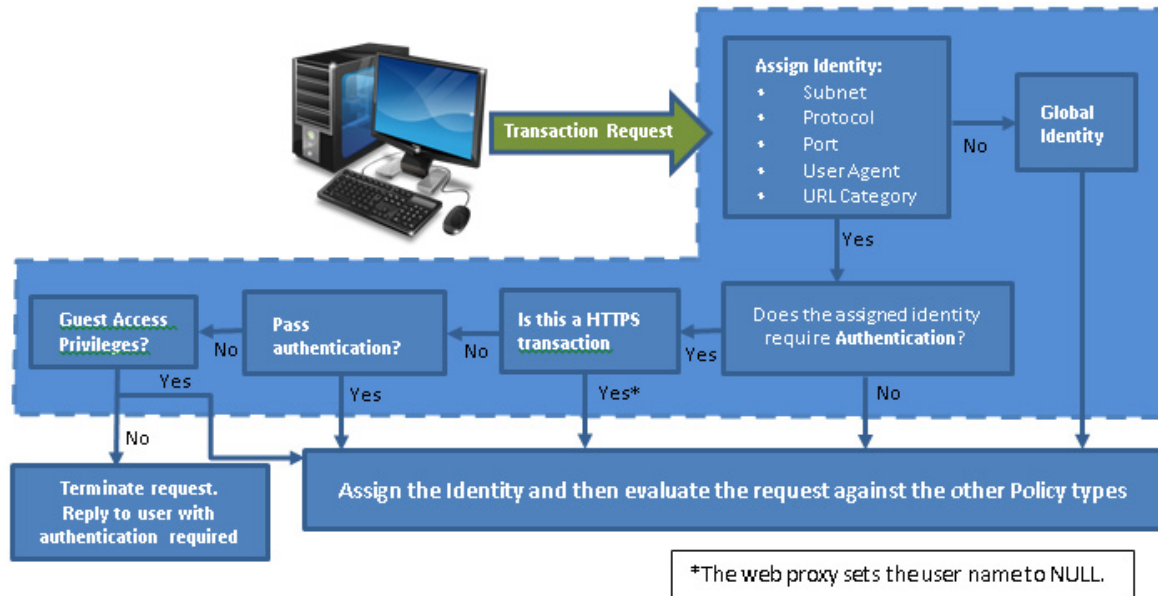


Figure 7-2 Transaction Request flow: Identities and Authentication - TranCookie-Based Surrogates



Troubleshooting Identities

- Policy Problems, page A-7
- Policy is Never Applied, page A-8

- [Policy Troubleshooting Tool: Policy Trace, page A-10](#)
- [Basic Authentication Problems, page A-2](#)
- [Upstream Proxy Problems, page A-13](#)
- [Upstream Proxy Problems, page A-13](#)
- [Policy is Never Applied, page A-8](#)



SaaS Access Control

- [Overview of SaaS Access Control, page 8-1](#)
- [Authenticate SaaS Users, page 8-2](#)
- [Configuring the Appliance as an Identity Provider, page 8-2](#)
- [Using SaaS Access Control and Multiple Web Security Appliances, page 8-4](#)
- [Creating SaaS Application Authentication Policies, page 8-4](#)
- [Configuring End-User Access to the Single Sign-On URL, page 8-6](#)

Overview of SaaS Access Control

The Web Security appliance uses the Security Assertion Markup Language (SAML) to authorize access to SaaS applications. It works with SaaS applications that are strictly compliant with SAML version 2.0.

Cisco SaaS Access Control allows you to:

- Control which users can access SaaS applications and from where.
- Quickly disable access to all SaaS applications when users are no longer employed by the organization.
- Reduce the risk of phishing attacks that ask users to enter their SaaS user credentials.
- Choose whether users are transparently signed in (single sign-on functionality) or prompted to enter their authentication user name and password.

SaaS Access Control only works with SaaS applications that require an authentication mechanism supported by the Web Security appliance. Currently, the Web Proxy uses the “PasswordProtectedTransport” authentication mechanism.

To enable SaaS Access Control, you must configure settings on both the Web Security appliance and the SaaS application:

Step 1	Configure the web security appliance as an identity provider.	Configuring the Appliance as an Identity Provider, page 8-2
Step 2	Create an authentication policy for the SaaS application.	Creating SaaS Application Authentication Policies, page 8-4

Step 3	Configure the SaaS application for single sign-on.	Configuring End-User Access to the Single Sign-On URL, page 8-6
Step 4	(Optional) Configuring multiple web security appliances	Using SaaS Access Control and Multiple Web Security Appliances, page 8-4

Authenticate SaaS Users

-
- Step 1** Configure the “PasswordProtectedTransport” value when you create a SaaS Application Authentication Policy using the Authentication Context setting
- Step 2** Choose “Automatic” as the Authentication Context setting.
-

Related topics

- [Creating SaaS Application Authentication Policies, page 8-4](#)

Certificates and Keys

When the browser prompts users to authenticate, the browser sends the authentication credentials to the Web Proxy using a secure HTTPS connection. The appliance uses its own certificate and private key to create an HTTPS connection with the client by default. Most browsers will warn users that the certificate is not valid. To prevent users from seeing the invalid certificate message, you can upload a certificate and key pair your organization uses.

Configuring the Appliance as an Identity Provider

When you configure the Web Security appliance as an identity provider, the settings you define apply to all SaaS applications it communicates with. The Web Security appliance uses a certificate and key to sign each SAML assertion it creates.

Before You Begin

- (Optional) Locate a certificate (PEM format) and key for signing SAML assertions.
- Upload the certificate to each SaaS application.

-
- Step 1** Choose **Security Services > Identity Provider for SaaS page**.
- Step 2** Click **Edit Settings**.
- Step 3** In the **Identity Provider Domain Name** field enter a virtual domain name.
- Step 4** In the **Identity Provider Entity ID** field enter text (a URI format based string is recommended)
- Step 5** Either upload or generate a certificate and key:

**Note**

If the appliance has both an uploaded certificate and key pair and a generated certificate and key pair, it only uses the certificate and key pair currently selected in the Signing Certificate section.

Method	Additional Steps
Uploaded certificate and key	<ol style="list-style-type: none"> 1. Click Use Uploaded Certificate and Key. 2. Click Browse for the Certificate field. <p>Note The Web Proxy uses the first certificate or key in the file. The certificate file must be in PEM format. DER format is not supported.</p> <ol style="list-style-type: none"> 3. Click Browse for the Key field. The private key must be unencrypted. <p>Note The key length must be 512, 1024, or 2048 bits. The private key file must be in PEM format. DER format is not supported.</p> <ol style="list-style-type: none"> 4. Click Upload Files. 5. Click Download Certificate to transfer the certificate to the SaaS applications with which the Web Security appliance will communicate. 6. Submit and Commit Changes
Generated certificate and key	<ol style="list-style-type: none"> 1. Click Use Generated Certificate and Key. 2. Click Generate New Certificate and Key. 3. In the Generate Certificate and Key dialog box, enter the information to display in the signing certificate. <p>Note You can enter any ASCII character except the forward slash (/) in the Common Name field.</p> <ol style="list-style-type: none"> 4. Click Generate. 5. Click Download Certificate to transfer the certificate to the SaaS applications with which the Web Security appliance will communicate. 6. (Optional) Click the Download Certificate Signing Request (DCSR) link to submit it to a certificate authority (CA). After you receive a signed certificate from the CA, click Browse and navigate to the signed certificate location. Click Upload File. 7. Submit and Commit Changes

Step 6 After you choose which certificate and key to use for signing SAML assertions, upload the certificate to each SaaS application.

Step 7 Make note of the settings when you configure the appliance as an identity provider. Some of these settings must be used when configuring the SaaS application for single sign-on.

Related Topics

- [Configuring End-User Access to the Single Sign-On URL, page 8-6](#)

Using SaaS Access Control and Multiple Web Security Appliances

Before you begin

- [Configure the Appliance as an Identity Provider, page 15-2](#)

-
- Step 1** Configure the same Identity Provider Domain Name for each Web Security appliance.
- Step 2** Configure the same Identity Provider Entity ID for each Web Security appliance.
- Step 3** Upload the same certificate and private key to each appliance on the **Security Services > Identity Provider for SaaS** page.
- Step 4** Upload this certificate to each SaaS application you configure.
-

Creating SaaS Application Authentication Policies

Before you begin

- Create associated identities.
- Configure Identity Provider, see [Configuring the Appliance as an Identity Provider, page 8-2](#).
- Create an Authentication Realm, [Authentication Realms, page 6-3](#).

-
- Step 1** Choose **Web Security Manager > SaaS Policies**.
- Step 2** Click **Add Application**.
- Step 3** Configure the settings:

Property	Description
Application Name	Enter a name to identify the SaaS application for this policy, each application name must be unique. The Web Security appliance uses the application name to generate a single sign-on URL.
Description	(Optional) Enter a description for this SaaS policy.

Property	Description
Metadata for Service Provider	<p>Configure the metadata that describes the service provider referenced in this policy. You can either describe the service provider properties manually or upload a metadata file provided by the SaaS application.</p> <p>The Web Security appliance uses the metadata to determine how to communicate with the SaaS application (service provider) using SAML. Contact the SaaS application to learn the correct settings to configure the metadata.</p> <p>When you manually configure the metadata information, configure the following values:</p> <ul style="list-style-type: none"> • Service Provider Entity ID. Enter the text (typically in URI format) the SaaS application uses to identify itself as a service provider. • Name ID Format. Choose from the drop-down list the format the appliance should use to identify users in the SAML assertion it sends to service providers. The value you enter here must match the corresponding setting configured on the SaaS application. • Assertion Consumer Service Location. Enter the URL to where the Web Security appliance should send the SAML assertion it creates. Read the SaaS application documentation to determine that correct URL to use (also known as the login URL). <p>Note The metadata file is an XML document following the SAML standard that describes a service provider instance. Not all SaaS applications use metadata files, but for those that do, contact the SaaS application provider for the file.</p>
Authentication	<p>Choose the authentication realm or authentication sequence the Web Proxy should use to authenticate users accessing this SaaS application. Users must be a member of the authentication realm or authentication sequence to successfully access the SaaS application.</p> <p>In the SaaS SSO Authentication Prompt section, choose how to sign users into the SaaS application:</p> <ul style="list-style-type: none"> • Always prompt users for their local authentication credentials. • Prompt users for their local authentication credentials if the Web Proxy obtained their user names using transparent user identification. • Automatically sign in users to the SaaS application using their local authentication credentials.
SAML User Name Mapping	<p>Specify how the Web Proxy should represent user names to the service provider in the SAML assertion. You can pass the user names as they are used inside your network (no mapping), or you can change the internal user names into a different format using one of the following methods:</p> <ul style="list-style-type: none"> • LDAP query. The user names sent to the service provider are based on one or more LDAP query attributes. Enter an expression containing LDAP attribute fields and optional custom text. You must enclose attribute names in angled brackets. You can include any number of attributes. For example, for the LDAP attributes “user” and “domain,” you could enter <user>@<domain>.com. • Fixed Rule mapping. The user names sent to the service provider are based on the internal user name with a fixed string added before or after the internal user name. Enter the fixed string and %s for the internal user name.

Property	Description
SAML Attribute Mapping	(Optional) You can provide to the SaaS application additional information about the internal users from the LDAP authentication server if required by the SaaS application. Map each LDAP server attribute to a SAML attribute.
Authentication Context	From the Authentication drop-down list, choose the authentication mechanism the Web Proxy uses to authenticate its internal users. Note The authentication context informs the service provider which authentication mechanism the identity provider used to authenticate the internal users. Some service providers require a particular authentication mechanism to allow users to access the SaaS application. If a service provider requires an authentication context that is not supported by an identity provider, users cannot access the service provider using single sign-on from the identity provider.

Step 4 Submit and Commit Changes.

Next Steps

- Download the certificate and install it on the application website. **Security Services > Identity Provider for SaaS > Edit Settings > click Download Certificate**
- Set up the single sign-on settings on the SaaS application side, using the same parameters to configure the application.

Configuring End-User Access to the Single Sign-On URL

After you configure the Web Security appliance as an identity provider and create a SaaS Application Authentication Policy for the SaaS application, the appliance creates a single sign-on URL (SSO URL). The Web Security appliance uses the application name configured in the SaaS Application Authentication Policy to generate the single sign-on URL. The single sign-on URL format is:

http://IdentityProviderDomainName/SSOURL/ApplicationName

-
- Step 1** Obtain the single sign-on URL from the **Web Security Manager > SaaS Policies** page
 - Step 2** Make the URL available to end-users depending on which flow type
 - Step 3** If you choose Identity provider initiated flow, the appliance redirects users to the SaaS application
 - Step 4** If you choose Service Provider initiated flows, you must configure this URL in the SaaS application.
 - Always prompt SaaS users for proxy authentication. After entering valid credentials, users are logged into the SaaS application.
 - Transparently sign in SaaS users. Users are logged into the SaaS application automatically.



Note

To achieve single sign-on behavior using explicit forward requests for all authenticated users when the appliance is deployed in transparent mode, select “**Apply same surrogate settings to explicit forward requests**” when you configure the Identity group.



CHAPTER 9

Classify URLs for Policy Application

- [Overview of Categorizing URL Transactions, page 9-1](#)
- [Configuring the URL Filtering Engine, page 9-4](#)
- [Managing Updates to the Set of URL Categories, page 9-4](#)
- [Filtering Transactions Using URL Categories, page 9-9](#)
- [Creating and Editing Custom URL Categories, page 9-13](#)
- [Filtering Adult Content, page 9-15](#)
- [Redirecting Traffic in the Access Policies, page 9-17](#)
- [Warning Users and Allowing Them to Continue, page 9-17](#)
- [Creating Time Based URL Filters, page 9-19](#)
- [Viewing URL Filtering Activity, page 9-19](#)
- [Regular Expressions, page 9-20](#)
- [URL Category Descriptions, page 9-22](#)

Overview of Categorizing URL Transactions

Using policy groups, you can create secure policies that control access to web sites containing questionable content. The sites that are blocked, allowed, or decrypted depend on the categories you select when setting up category blocking for each policy group. To control user access based on a URL category, you must enable Cisco Web Usage Controls. This is a multi-layered URL filtering engine that uses domain prefixes and keyword analysis to categorize URLs.

You can use URL categories when performing the following tasks:

Option	Method
Define policy group membership	Matching URLs to URL Categories, page 9-3
Control access to HTTP, HTTPS, and FTP requests	Filtering Transactions Using URL Categories, page 9-9
Create user defined custom URL categories that specify specific hostnames and IP addresses	Creating and Editing Custom URL Categories, page 9-13

Categorization of Failed URL Transactions

The Dynamic Content Analysis engine categorizes URLs when controlling access to websites in Access Policies only. It does not categorize URLs when determining policy group membership or when controlling access to websites using Decryption or Cisco Data Security Policies. This is because the engine works by analyzing the response content from the destination server, so it cannot be used on decisions that must be made at request time before any response is downloaded from the server.

If the web reputation score for an uncategorized URL is within the WBRS ALLOW range, AsyncOS allows the request without performing Dynamic Content Analysis.

After the Dynamic Content Analysis engine categorizes a URL, it stores the category verdict and URL in a temporary cache. This allows future transactions to benefit from the earlier response scan and be categorized at request time instead of at response time.

Enabling the Dynamic Content Analysis engine can impact transaction performance. However, most transactions are categorized using the Cisco Web Usage Controls URL categories database, so the Dynamic Content Analysis engine is usually only called for a small percentage of transactions.

Enabling the Dynamic Content Analysis Engine

-
- Step 1** Choose **Security Services > Acceptable Use Controls**.
 - Step 2** Enable the Cisco Web Usage Controls.
 - Step 3** **Click** to enable the Dynamic Content Analysis engine.
 - Step 4** **Submit** and **Commit Changes**.
-



Note

It is possible for an Access Policy, or an Identity used in an Access Policy, to define policy membership by a predefined URL category and for the Access Policy to perform an action on the same URL category. The URL in the request can be uncategorized when determining Identity and Access Policy group membership, but must be categorized by the Dynamic Content Analysis engine after receiving the server response. Cisco Web Usage Controls ignores the category verdict from the Dynamic Content Analysis engine and the URL retains the “uncategorized” verdict for the remainder of the transaction. Future transactions will still benefit from the new category verdict.

Uncategorized URLs

An uncategorized URL is a URL that does not match any pre-defined URL category or *included* custom URL category.



Note

When determining policy group membership, a custom URL category is considered included only when it is selected for policy group membership.

All transactions resulting in unmatched categories are reported on the Reporting > URL Categories page as “Uncategorized URLs.” A large number of uncategorized URLs are generated from requests to web sites within the internal network. Cisco recommends using custom URL categories to group internal

URLs and allow all requests to internal web sites. This decreases the number of web transactions reported as “Uncategorized URLs” and instead reports internal transactions as part of “URL Filtering Bypassed” statistics.

Related Topics

- [Understanding Unfiltered and Uncategorized Data, page 9-19.](#)
- [Creating and Editing Custom URL Categories, page 9-13.](#)

Matching URLs to URL Categories

When the URL filtering engine matches a URL category to the URL in a client request, it first evaluates the URL against the custom URL categories *included* in the policy group. If the URL in the request does not match an included custom category, the URL filtering engine compares it to the predefined URL categories. If the URL does not match any included custom or predefined URL categories, the request is uncategorized.



Note

When determining policy group membership, a custom URL category is considered included only when it is selected for policy group membership.



Tip

To see what category a particular web site is assigned to, go to the URL in [Reporting Uncategorized and Misclassified URLs, page 9-3.](#)

Related Topics

- [Uncategorized URLs, page 9-2.](#)

Reporting Uncategorized and Misclassified URLs

You can report uncategorized and misclassified URLs to Cisco. Cisco provides a URL submission tool on its website that allows you to submit multiple URLs simultaneously:

`https://securityhub.cisco.com/web/submit_urls`

To check the status of submitted URLs, click the **Status on Submitted URLs** tab on this page. You can also use the URL submission tool to look up the assigned URL category for any URL.

URL Categories Database

The category that a URL falls into is determined by a filtering categories database. The Web Security appliance collects information and maintains a separate database for each URL filtering engine. The filtering categories databases periodically receive updates from the Cisco update server (`https://update-manifests.ironport.com`).

The URL categories database includes many different factors and sources of data internal to Cisco and from the Internet. One of the factors occasionally considered, heavily modified from the original, is information from the Open Directory Project.

**Tip**

To see what category a particular web site is assigned to, go to the URL in [Reporting Uncategorized and Misclassified URLs](#), page 9-3.

Related Topics

- [Manually Updating Security Service Components](#), page 21-27.

Configuring the URL Filtering Engine

By default, the Cisco Web Usage Controls URL filtering engine is enabled in the System Setup Wizard.

-
- Step 1** Choose **Security Services > Acceptable Use Controls**.
- Step 2** Click **Edit Global Settings**.
- Step 3** Verify the **Enable Acceptable Use Controls** property is enabled.
- Step 4** Choose whether or not to enable the Dynamic Content Analysis Engine.
- Step 5** Choose the default action the Web Proxy should use when the URL filtering engine is unavailable, either Monitor or Block. Default is Monitor.
- Step 6** **Submit** and **Commit Changes**.
-

Managing Updates to the Set of URL Categories

The set of predefined URL categories may occasionally be updated in order to accommodate new web trends and evolving usage patterns. Updates to the URL category set are distinct from the changes that add new URLs and re-map misclassified URLs. Category set updates may change configurations in your existing policies and therefore require action. URL category set updates may occur between product releases; an AsyncOS upgrade is not required.

Information is available from:

http://www.cisco.com/en/US/products/ps10164/prod_release_notes_list.html.

Take the following actions:

When to Act	Method
Before updates occur (Do these tasks as part of your initial setup)	Understanding the Impacts of URL Category Set Updates , page 9-5 Controlling Updates to the URL Category Set , page 9-7 Default Settings for New and Changed Categories , page 9-8 Receiving Alerts About Category and Policy Changes , page 9-8
After updates occur	Responding to Alerts about URL Category Set Updates , page 9-8

Understanding the Impacts of URL Category Set Updates

URL category set updates can have the following impacts on existing Access Policies, Decryption Policies, and Cisco Data Security policies, and on Identities:

- [Effects of URL Category Set Changes on Policy Group Membership, page 9-5](#)
- [Effects of URL Category Set Updates on Filtering Actions in Policies, page 9-5](#)

Effects of URL Category Set Changes on Policy Group Membership

This section applies to all policy types with membership that can be defined by URL category, and to Identities. When policy group membership is defined by URL category, changes to the category set may have the following effects:

- If the sole criterion for membership is a deleted category, the policy or identity is disabled.
- If membership in any policy is defined by a URL category that changes, and if this causes ACL list changes, the web proxy will restart.

Effects of URL Category Set Updates on Filtering Actions in Policies

URL category set updates can change policy behavior in the following ways:

Change	Effect on Policies and Identities
A new category can be added	For each policy, the default action for newly-added categories is the action specified for Uncategorized URLs for that policy.
A category can be deleted	The action associated with the deleted category is deleted. If the policy depended exclusively on the deleted category, the policy is disabled. If a policy depends on an identity that depended exclusively on a deleted category, the policy will be disabled.
A category can be renamed	No change to the behavior of the existing policy.
A category can split	A single category can become multiple new categories. Both new categories have the action associated with the original category.

Change	Effect on Policies and Identities
Two or more existing categories can merge	<p>If all original categories in a policy had the same action assigned, the merged category has the same action as the original categories. If all original categories were set to “Use Global Setting” then the merged category is also set to “Use Global Setting.”</p> <p>If the policy had different actions assigned to the original categories, the action assigned to the merged category depends on the Uncategorized URLs setting in that policy:</p> <ul style="list-style-type: none"> • If Uncategorized URLs is set to Block (or “Use Global Setting” when the global setting is Block), then the most restrictive action among the original categories is applied to the merged category. • If Uncategorized URLs is set to any action other than Block (or “Use Global Setting” when the global setting is anything other than Block), then the least restrictive action among the original categories is applied to the merged category. <p>In this case, sites that were previously blocked may now be accessible to users.</p> <p>If policy membership is defined by URL category, and some of the categories involved in the merge, or the Uncategorized URLs action, are not included in the policy membership definition, then the values in the Global Policy are used for the missing items.</p> <ul style="list-style-type: none"> • The order of restrictiveness is as follows (not all actions are available for all policy types):Block • Drop • Decrypt • Warn • Time-based • Monitor • Pass Through <p>Note Time-based policies that are based on merged categories adopt the action associated with any one of the original categories. (In time-based policies, there may be no obviously most- or least-restrictive action.)</p>

Related Topics

- [Merged Categories - Examples, page 9-6.](#)

Merged Categories - Examples

Some examples of merged categories, based on settings on the URL Filtering page for the policy:

Original Category 1	Original Category 2	Uncategorized URLs	Merged Category
Monitor	Monitor	(Not Applicable)	Monitor
Block	Block	(Not Applicable)	Block
Use Global Settings	Use Global Settings	(Not Applicable)	Use Global Settings
Warn	Block	Monitor Use the least restrictive among the original categories.	Warn

Original Category 1	Original Category 2	Uncategorized URLs	Merged Category
Monitor	<ul style="list-style-type: none"> Block or Use Global Settings, when Global is set to Block 	<ul style="list-style-type: none"> Block or Use Global Setting, when Global is set to Block <p>Use the most restrictive among the original categories.</p>	Block
Block	<ul style="list-style-type: none"> Monitor or Use Global Settings, when Global is set to Monitor 	<ul style="list-style-type: none"> Monitor or Use Global Setting, when Global is set to Monitor <p>Use the least restrictive among the original categories.</p>	Monitor
For policies in which membership is defined by URL category: Monitor	An action for this category is not specified in this policy, but the value in the Global Policy for this category is Block	An action for Uncategorized URLs is not specified in this policy, but the value in the Global Policy for Uncategorized URLs is Monitor	Monitor

Controlling Updates to the URL Category Set

By default, URL category set updates to occur automatically. These updates may change existing policy configurations, so you may prefer to disable all automatic updates.

Option	Method
If you disable updates, you will need to manually update all services listed in the Update Servers (list) section of the System Administration > Upgrade and Update Settings page	Manually Updating the URL Category Set, page 9-7 and Manually Updating Security Service Components, page 21-27
Disabling all automatic updates	Configuring Upgrade and Service Update Settings, page 21-31.



Note

If you use the CLI, disable updates by setting the update interval to zero (0)

Manually Updating the URL Category Set



Note

Do not interrupt an update in progress.

If you have disabled automatic updates, you can manually update the set of URL categories at your convenience.

-
- Step 1** Choose **Security Services > Acceptable Use Controls**.
- Step 2** Determine whether an update is available:
Look at the “Cisco Web Usage Controls - Web Categorization Categories List” item in the Acceptable Use Controls Engine Updates table.
- Step 3** To update, click **Update Now**.
-

Default Settings for New and Changed Categories

URL category set updates may change the behavior of your existing policies. You should specify default settings for certain changes when you configure your policies, so that they are ready when URL category set updates occur. When new categories are added, or existing categories merge into a new category, the default action for these categories for each policy are affected by the Uncategorized URLs setting in that policy.

Verifying Existing Settings and/or Making Changes

-
- Step 1** Choose **Web Security Manager**.
- Step 2** For each Access Policy, Decryption Policy, and Cisco Data Security policy click the **URL Filtering link**.
- Step 3** Check the selected setting for Uncategorized URLs.
-

Related Topics

- [Effects of URL Category Set Updates on Filtering Actions in Policies, page 17-6.](#)

Receiving Alerts About Category and Policy Changes

Category set updates trigger two types of alerts:

- Alerts about category changes
- Alerts about policies that have changed or been disabled as a result of category set changes.

-
- Step 1** Choose **System Administration > Alerts**.
- Step 2** Click **Add Recipient** and add email address (or multiple email addresses).
- Step 3** Decide which **Alert Types** and **Alert Severities** to receive.
- Step 4** **Submit** and **Commit Changes**.
-

Responding to Alerts about URL Category Set Updates

When you receive an alert about category set changes, you should do the following:

- Check policies and identities to be sure that they still meet your policy goals after category merges, additions, and deletions, and
- Consider modifying policies and identities to benefit from new categories and the added granularity of split categories.

Related Topics

- [Understanding the Impacts of URL Category Set Updates, page 9-5](#)

Filtering Transactions Using URL Categories

The URL filtering engine configured allows you to filter transactions in Access, Decryption, and Data Security Policies. When you configure URL categories for policy groups, you can configure actions for custom URL categories, if any are defined, and predefined URL categories.

The URL filtering actions you can configure depends on the type of policy group:

Option	Method
Access Policies	Configuring URL Filters for Access Policy Groups, page 9-9
Decryption Policies	Configuring URL Filters for Decryption Policy Groups, page 9-11
Cisco Data Security Policies	Configuring URL Filters for Data Security Policy Groups, page 9-12

Configuring URL Filters for Access Policy Groups

You can configure URL filtering for user defined Access Policy groups and the Global Policy Group.

-
- Step 1** Choose **Web Security Manager > Access Policies**.
- Step 2** Click the link in the policies table under the URL Filtering column for the policy group you want to edit.
- Step 3** (Optional) In the Custom URL Category Filtering section, you can add custom URL categories on which to take action in this policy:
- Click **Select Custom Categories**.
 - Choose which custom URL categories to include in this policy and click **Apply**.

Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.

Step 4 In the **Custom URL Category Filtering** section, choose an action for each included custom URL category.

Action	Description
Use Global Setting	<p>Uses the action for this category in the Global Policy Group. This is the default action for user defined policy groups.</p> <p>Applies to user defined policy groups only.</p> <p>Note When a custom URL category is excluded in the global Access Policy, then the default action for included custom URL categories in user defined Access Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global Access Policy.</p>
Redirect	Redirects traffic originally destined for a URL in this category to a location you specify. When you choose this action, the Redirect To field appears. Enter a URL to which to redirect all traffic.
Allow	<p>Always allows client requests for web sites in this category.</p> <p>Allowed requests bypass all further filtering and malware scanning.</p> <p>Only use this setting for trusted web sites. You might want to use this setting for internal sites.</p>
Monitor	The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the client request against other policy group control settings, such as web reputation filtering.
Warn	The Web Proxy initially blocks the request and displays a warning page, but allows the user to continue by clicking a hypertext link in the warning page.
Block	The Web Proxy denies transactions that match this setting.
Time-Based	The Web Proxy blocks or monitors the request during the time ranges you specify.

Step 5 In the **Predefined URL Category Filtering** section, choose one of the following actions for each category:

- Use Global Settings
- Monitor
- Warn
- Block
- Time-Based

Step 6 In the **Uncategorized URLs** section, choose the action to take for client requests to web sites that do not fall into a predefined or custom URL category. This setting also determines the default action for new and merged categories resulting from URL category set updates.

Step 7 **Submit** and **Commit Changes**.

Related Topics

- [Redirecting Traffic in the Access Policies, page 9-17.](#)
- [Warning Users and Allowing Them to Continue, page 9-17](#)

- [Creating and Editing Custom URL Categories, page 9-13](#)
- [Effects of URL Category Set Updates on Filtering Actions in Policies, page 9-5](#)

Configuring URL Filters for Decryption Policy Groups

You can configure URL filtering for user defined Decryption Policy groups and the global Decryption Policy group.

-
- Step 1** Choose **Web Security Manager > Decryption Policies**.
- Step 2** Click the link in the policies table under the URL Categories column for the policy group you want to edit.
- Step 3** (Optional) In the Custom URL Category Filtering section, you can add custom URL categories on which to take action in this policy:
- Click **Select Custom Categories**.
 - Choose which custom URL categories to include in this policy and click **Apply**.
Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.
The custom URL categories included in the policy appear in the Custom URL Category Filtering section.
- Step 4** Choose an action for each custom and predefined URL category.

Action	Description
Use Global Setting	Uses the action for this category in the global Decryption Policy group. This is the default action for user defined policy groups. Applies to user defined policy groups only. When a custom URL category is excluded in the global Decryption Policy, then the default action for included custom URL categories in user defined Decryption Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global Decryption Policy.
Pass Through	Passes through the connection between the client and the server without inspecting the traffic content.
Monitor	The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the client request against other policy group control settings, such as web reputation filtering.
Decrypt	Allows the connection, but inspects the traffic content. The appliance decrypts the traffic and applies Access Policies to the decrypted traffic as if it were a plain text HTTP connection. By decrypting the connection and applying Access Policies, you can scan the traffic for malware.
Drop	Drops the connection and does not pass the connection request to the server. The appliance does not notify the user that it dropped the connection.



Note If you want to *block* a particular URL category for HTTPS requests, choose to decrypt that URL category in the Decryption Policy group and then choose to block the same URL category in the Access Policy group.

Step 5 In the Uncategorized URLs section, choose the action to take for client requests to web sites that do not fall into a predefined or custom URL category.

This setting also determines the default action for new and merged categories resulting from URL category set updates.

Step 6 **Submit** and **Commit Changes**.

Configuring URL Filters for Data Security Policy Groups

You can configure URL filtering for user defined Data Security Policy groups and the Global Policy Group.

Step 1 Choose **Web Security Manager > Cisco Data Security**.

Step 2 Click the link in the policies table under the URL Categories column for the policy group you want to edit.

Step 3 (Optional) In the Custom URL Category Filtering section, you can add custom URL categories on which to take action in this policy:

- a. Click **Select Custom Categories**.
- b. Choose which custom URL categories to include in this policy and click **Apply**.

Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.

Step 4 In the Custom URL Category Filtering section, choose an action for each custom URL category.

Action	Description
Use Global Setting	<p>Uses the action for this category in the Global Policy Group. This is the default action for user defined policy groups.</p> <p>Applies to user defined policy groups only.</p> <p>When a custom URL category is excluded in the global Cisco Data Security Policy, then the default action for included custom URL categories in user defined Cisco Data Security Policies is Monitor instead of Use Global Settings. You cannot choose Use Global Settings when a custom URL category is excluded in the global Cisco Data Security Policy.</p>
Allow	<p>Always allows upload requests for web sites in this category. Applies to custom URL categories only.</p> <p>Allowed requests bypass all further data security scanning and the request is evaluated against Access Policies.</p> <p>Only use this setting for trusted web sites. You might want to use this setting for internal sites.</p>
Monitor	The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the upload request against other policy group control settings, such as web reputation filtering.
Block	The Web Proxy denies transactions that match this setting.

Step 5 In the Predefined URL Category Filtering section, choose one of the following actions for each category:

- Use Global Settings
- Monitor
- Block

Step 6 In the Uncategorized URLs section, choose the action to take for upload requests to web sites that do not fall into a predefined or custom URL category. This setting also determines the default action for new and merged categories resulting from URL category set updates.

Step 7 **Submit and Commit Changes.**

Related Topics

- [Effects of URL Category Set Updates on Filtering Actions in Policies, page 9-5.](#)

Creating and Editing Custom URL Categories

You can also create user defined custom URL categories that specify specific hostnames and IP addresses. In addition, you can edit and delete existing URL categories. When you include these custom URL categories in the same Access, Decryption, or Cisco Data Security Policy group and define different actions to each category, the action of the higher included custom URL category takes effect.

**Note**

The Web Security appliance uses the first four characters of custom URL category names preceded by “c_” in the access logs. Consider the custom URL category name if you use Sawmill for to parse the access logs. If the first four characters of the custom URL category include a space, Sawmill for cannot properly parse the access log entry. Instead, only use supported characters in the first four characters if you will use Sawmill for to parse the access logs. If you want to include the full name of a custom URL category in the access logs, add the %XF format specifier to the access logs.

Step 1 Choose **Web Security Manager > Custom URL Categories**.

Step 2 To create a custom URL category, click **Add Custom Category**. To edit an existing custom URL category, click the name of the URL category.

Step 3 Enter the settings in the table below for the custom URL category.

Setting	Description
Category Name	Enter a name for the URL category. This name appears when you configure URL filtering for policy groups.
List Order	Choose the order in the list of custom URL categories to place this category. Enter “1” for the topmost URL category. The URL filtering engine evaluates a client request against the custom URL categories in the order specified.
Sites	Enter one or more addresses that belong in the custom category. You can enter multiple addresses separated by line breaks or commas.
Advanced: Regular Expressions	You can use regular expressions to specify multiple web servers that match the pattern you enter. Note The URL filtering engine compares URLs with addresses entered in the Sites field first. If the URL of a transaction matches an entry in the Sites field, it is not compared to any expression entered here.

Step 4 (Optional) Click **Sort URLs** to sort all addresses in the Sites field.

**Note**

Once you sort the addresses, you cannot retrieve their original order.

Step 5 **Submit** and **Commit Changes**.

Related Topics

- [Regular Expressions, page 9-20.](#)
- [Customizing Access Logs, page 20-17.](#)

Filtering Adult Content

You can configure the Web Security appliance to filter adult content from some web searches and websites. To enforce safe search and site content ratings, the AVC engine takes advantage of the safe mode feature implemented at a particular website by rewriting URLs and/or web cookies to force the safety mode to be on.

The following features filter adult content:

Option	Description
Enforce safe searches	You can configure the Web Security appliance so that outgoing search requests appear to search engines as safe search requests. This can prevent users from bypassing acceptable use policies using search engines.
Enforce site content ratings	Some content sharing sites allow users to restrict their own access to the adult content on these sites by either enforcing their own safe search feature or blocking access to adult content, or both. This classification feature is commonly called content ratings.

**Note**

Any Access Policy that has either the safe search or site content ratings feature enabled is considered a safe browsing Access Policy.

Enforcing Safe Searches and Site Content Ratings

- Step 1** Choose **Web Security Manager > Access Policies**.
- Step 2** Click the link under the URL Categories column for an Access Policy group or the Global Policy Group.
- Step 3** When editing a user-defined Access Policy, choose **Define Content Filtering Custom Settings** in the Content Filtering section.
- Step 4** Click the **Enable Safe Search** check box to enable the safe search feature.
- Step 5** Choose whether to block users from search engines that are not currently supported by the Web Security appliance safe search feature.
- Step 6** Click the **Enable Site Content Rating** check box to enable the site content ratings feature.
- Step 7** Choose whether to block all adult content from the supported content ratings websites or to display the end-user URL filtering warning page.

**Note**

When the URL of one of the supported search engines or supported content ratings websites is included in a custom URL category with the Allow action applied, no search results are blocked and all content is visible.

Step 8 Submit and Commit Changes.**Related Topics**

- [Warning Users and Allowing Them to Continue, page 9-17.](#)
- [Controlling Access to Web Applications, page 17-18](#)

Logging Adult Content Access

By default, the access logs include a safe browsing scanning verdict inside the angled brackets of each entry. The safe browsing scanning verdict indicates whether or not either the safe search or site content ratings feature was applied to the transaction. You can also add the safe browsing scanning verdict variable to the access logs or W3C access logs:

- Access logs: %XS
- W3C access logs: x-request-rewrite

Value	Description
ensrch	The original client request was unsafe and the safe search feature was applied.
enrct	The original client request was unsafe and the site content ratings feature was applied.
unsupp	The original client request was to an unsupported search engine.
err	The original client request was unsafe, but neither the safe search nor the site content ratings feature could be applied due to an error.
-	Neither the safe search nor the site content ratings feature was applied to the client request because the features were bypassed (for example, the transaction was allowed in a custom URL category) or the request was made from an unsupported application.

Requests blocked due to either the safe search or site content rating features, use one of the following ACL decision tags in the access logs:

- BLOCK_SEARCH_UNSAFE
- BLOCK_CONTENT_UNSAFE
- BLOCK_UNSUPPORTED_SEARCH_APP
- BLOCK_CONTINUE_CONTENT_UNSAFE

Related Topics

- [ACL Decision Tags, page 20-33.](#)

Redirecting Traffic in the Access Policies

You can configure the Web Security appliance to redirect traffic originally destined for a URL in a custom URL category to a location you specify. This allows you to redirect traffic at the appliance instead of at the destination server. You can redirect traffic for a custom Access Policy group or the Global Policy Group

Before you Begin

- To redirect traffic you must define at least one custom URL category.

-
- Step 1** Choose **Web Security Manager > Access Policies**.
- Step 2** Click the link under the URL Categories column for an Access Policy group or the Global Policy Group.
- Step 3** In the Custom URL Category Filtering section, click **Select Custom Categories**.
- Step 4** In the **Select Custom Categories for this Policy** dialog box, choose **Include in policy** for the custom URL category you want to redirect.
- Step 5** Click **Apply**.
- Step 6** Click the **Redirect** column for the custom category you want to redirect.
- Step 7** Enter the URL to which you want to redirect traffic in the **Redirect To** field for the custom category.
- Step 8** **Submit** and **Commit Changes**.



Note

Beware of infinite loops when you configure the appliance to redirect traffic.

Related Topics

- [Creating and Editing Custom URL Categories, page 9-13](#)

Logging and Reporting

When you redirect traffic, the access log entry for the originally requested website has an ACL tag that starts with REDIRECT_CUSTOMCAT. Later in the access log (typically the next line) appears the entry for the website to which the user was redirected.

The reports displayed on the Reporting tab display redirected transactions as “Allowed.”

Warning Users and Allowing Them to Continue

You can warn users that a site does not meet the organization’s acceptable use policies. Users are tracked in the access log by user name if authentication has made a user name available, and tracked by IP address if no user name is available.

You can warn and allow users to continue using one of the following methods:

- Choose the Warn action for a URL category in an Access Policy group or

- Enable the site content ratings feature and warn users that access adult content instead of blocking them.

Configuring Settings for the End-User Filtering Warning Page

- Step 1** Choose **Security Services > End-User Notification**.
- Step 2** Click **Edit Settings**.
- Step 3** Configure the following settings on the **End-User Filtering Warning** page:

Option	Method
Time Between Warning	<p>The Time Between Warning determines how often the Web Proxy displays the end-user URL filtering warning page for each URL category per user.</p> <p>This setting applies to users tracked by username and users tracked by IP address.</p> <p>Specify any value from 30 to 2678400 seconds (one month). Default is 1 hour (3600 seconds).</p>
Custom Message	<p>The custom message is text you enter that appears on every end-user URL filtering warning page.</p> <p>Include some simple HTML tags to format the text.</p>

- Step 4** Click **Submit**.



Note

The warn and continue feature only works for HTTP and decrypted HTTPS transactions. It does not work with native FTP transactions.



Note

When the URL filtering engine warns users for a particular request, it provides a warning page that the Web Proxy sends to the end user. (However, not all websites display the warning page to the end user. When this happens, users are blocked from the URL that is assigned the Warn option without being given the chance to continue accessing the site anyway.

Related Topics

- [Filtering Adult Content, page 9-15](#)
- [Custom Text in Notification Pages, page 16-13](#)
- [Configuring the End-User URL Filtering Warning Page, page 16-12](#)

Creating Time Based URL Filters

You can configure how the Web Security appliance handles requests for URLs in particular categories differently based on time and day.

Before you Begin

Go to the **Web Security Manager > Defined Time Range** page to define at least one time range.

-
- Step 1** Choose **Web Security Manager > Access Policies**.
 - Step 2** Click the link in the policies table under the URL Categories column for the policy group you want to edit.
 - Step 3** Select **Time-Based** for the custom or predefined URL category you want to configure based on time range.
 - Step 4** In the **In Time Range** field, choose the defined time range to use for the URL category.
 - Step 5** In the **Action** field, choose the action to enact on transactions in this URL category during the defined time range.
 - Step 6** In the **Otherwise** field, choose the action to enact on transactions in this URL category *outside* the defined time range.
 - Step 7** **Submit** and **Commit Changes**.
-

Related Topics

- [Limiting Access by Time of Day, page 10-13](#)

Viewing URL Filtering Activity

The **Reporting > URL Categories** page provides a collective display of URL statistics that includes information about top URL categories matched and top URL categories blocked. This page displays category-specific data for bandwidth savings and web transactions.

Related Topics

- [Generate Reports to Monitor End-user Activity, page 17-1](#)

Understanding Unfiltered and Uncategorized Data

When viewing URL statistics on the **Reporting > URL Categories** page, it is important to understand how to interpret the following data:

Data Type	Description
URL Filtering Bypassed	Represents policy, port, and admin user agent blocking that occurs before URL filtering.
Uncategorized URL	Represents all transactions for which the URL filtering engine is queried, but no category is matched.

Access Log File

The access log file records the URL category for each transaction in the scanning verdict information section of each entry.

Related Topics

- [Monitor System Activity Through Logs, page 20-1.](#)
- [URL Category Descriptions, page 9-22.](#)

Regular Expressions

The Web Security appliance uses POSIX extended regular expression syntax, fully described by IEEE POSIX 1003.2. However, the appliance does not support using a backward slash to escape a forward slash. If you need to use a forward slash in a regular expression, type the forward slash without a backward slash.



Note

Technically, AsyncOS for Web uses the Flex regular expression analyzer. For more detailed information about how it reads regular expressions, see <http://flex.sourceforge.net/manual/Patterns.html>.

You can use regular expressions in the following locations:

- **Custom URL categories for Access Policies.** When you create a custom URL category to use with Access Policy groups, you can use regular expressions to specify multiple web servers that match the pattern you enter.
- **Custom user agents to block.** When you edit the applications to block for an Access Policy group, you can use regular expressions to enter specific user agents to block.



Note

Regular expressions that perform extensive character matching consume resources and can affect system performance. For this reason, regular expressions should be cautiously applied.

Related Topics

- [Creating and Editing Custom URL Categories, page 9-13](#)
- [Policy: Protocols and User Agents, page 9-13](#)

Forming Regular Expressions

Regular expressions are rules that typically use the word “matches” in the expression. They can be applied to match specific URL destinations or web servers. For example, the following regular expression matches any pattern containing blocksite.com:

```
\.blocksite\.com
```

Consider the following regular expression example:

```
server[0-9]\.example\.com
```

In this example, `server[0-9]` matches `server0`, `server1`, `server2`, ..., `server9` in the domain `example.com`.

In the following example, the regular expression matches files ending in .exe, .zip, and .bin in the downloads directory.

```
/downloads/.*\.(exe|zip|bin)
```

Avoid using regular expressions strings that are redundant because they can cause higher CPU usage on the Web Security appliance. A redundant regular expression is one that starts or ends with “.*”.

**Note**

You must enclose regular expressions that contain blank spaces or non-alphanumeric characters in ASCII quotation marks.

Regular Expression Character Table

Character	Description
.	Matches a single character.
*	Matches zero or more occurrences of the preceding regular expression. For example: [0-9]* matches any number of digits “.*” matches any arbitrary string of characters
^	Matches the beginning of a line as the first character of a regular expression.
\$	Matches the end of a line as the last character of a regular expression.
+	Matches one or more occurrences of the preceding regular expression.
?	Matches zero or one occurrence of the preceding regular expression.
	Matches the preceding regular expression or the following regular expression. For example: xly matches either x or y abclxyz matches either of the strings abc or xyz
[]	Matches the characters or digits that are enclosed within the brackets. For example: [a-z] matches any character between a and z [r-u] matches any of the characters r, s, t, or u [0-3] matches any of the single digits 0, 1, 2, 3
{ }	Specifies the number of times to match the previous pattern. For example: D{1,3} matches one to three occurrences of the letter D
()	Group characters in a regular expression. For example: (abc)* matches abc or abcabcabc
“...”	Literally interprets any characters enclosed within the quotation marks.
\	Escape character.

URL Category Descriptions

This section lists the URL categories for Cisco Web Usage Controls. The tables also include the abbreviated URL category names that may appear in the Web Reputation filtering and anti-malware scanning section of an access log file entry.



Note

In the access logs, the URL category abbreviations for Cisco Web Usage Controls include the prefix “IW_” before each abbreviation so that the “art” category becomes “IW_art.”

URL Category	Abbreviation	Code	Description	Example URLs
Adult	adlt	1006	Directed at adults, but not necessarily pornographic. May include adult clubs (strip clubs, swingers clubs, escort services, strippers); general information about sex, non-pornographic in nature; genital piercing; adult products or greeting cards; information about sex not in the context of health or disease.	www.adultentertainmentexpo.com www.adultnetline.com
Advertisements	adv	1027	Banner and pop-up advertisements that often accompany a web page; other advertising websites that provide advertisement content. Advertising services and sales are classified as “Business and Industry.”	www.adforce.com www.doubleclick.com
Alcohol	alc	1077	Alcohol as a pleasurable activity; beer and wine making, cocktail recipes; liquor sellers, wineries, vineyards, breweries, alcohol distributors. Alcohol addiction is classified as “Health and Nutrition.” Bars and restaurants are classified as “Dining and Drinking.”	www.samueladams.com www.whisky.com
Arts	art	1002	Galleries and exhibitions; artists and art; photography; literature and books; performing arts and theater; musicals; ballet; museums; design; architecture. Cinema and television are classified as “Entertainment.”	www.moma.org www.nga.gov
Astrology	astr	1074	Astrology; horoscope; fortune telling; numerology; psychic advice; tarot.	www.astro.com www.astrology.com
Auctions	auct	1088	Online and offline auctions, auction houses, and classified advertisements.	www.craigslist.com www.ebay.com
Business and Industry	busi	1019	Marketing, commerce, corporations, business practices, workforce, human resources, transportation, payroll, security and venture capital; office supplies; industrial equipment (process equipment), machines and mechanical systems; heating equipment, cooling equipment; materials handling equipment; packaging equipment; manufacturing: solids handling, metal fabrication, construction and building; passenger transportation; commerce; industrial design; construction, building materials; shipping and freight (freight services, trucking, freight forwarders, truckload carriers, freight and transportation brokers, expedited services, load and freight matching, track and trace, rail shipping, ocean shipping, road feeder services, moving and storage).	www.freightcenter.com www.staples.com
Chat and Instant Messaging	chat	1040	Web-based instant messaging and chat rooms.	www.icq.com www.meebo.com

URL Category Descriptions

URL Category	Abbreviation	Code	Description	Example URLs
Cheating and Plagiarism	plag	1051	Promoting cheating and selling written work, such as term papers, for plagiarism.	www.bestessays.com www.superiorpapers.com
Child Abuse Content	cprn	1064	Worldwide illegal child sexual abuse content.	—
Computer Security	csec	1065	Offering security products and services for corporate and home users.	www.computersecurity.com www.symantec.com
Computers and Internet	comp	1003	Information about computers and software, such as hardware, software, software support; information for software engineers, programming and networking; website design; the web and Internet in general; computer science; computer graphics and clipart. “Freeware and Shareware” is a separate category.	www.xml.com www.w3.org
Dating	date	1055	Dating, online personals, matrimonial agencies.	www.eharmony.com www.match.com
Digital Postcards	card	1082	Enabling sending of digital postcards and e-cards.	www.all-yours.net www.delivr.net
Dining and Drinking	food	1061	Eating and drinking establishments; restaurants, bars, taverns, and pubs; restaurant guides and reviews.	www.hideawaybrewpub.com www.restaurantrow.com
Dynamic and Residential	dyn	1091	IP addresses of broadband links that usually indicates users attempting to access their home network, for example for a remote session to a home computer.	http://109.60.192.55 http://dynamlink.co.jp http://ipadsl.net
Education	edu	1001	Education-related, such as schools, colleges, universities, teaching materials, and teachers’ resources; technical and vocational training; online training; education issues and policies; financial aid; school funding; standards and testing.	www.education.com www.greatschools.org
Entertainment	ent	1093	Details or discussion of films; music and bands; television; celebrities and fan websites; entertainment news; celebrity gossip; entertainment venues. Compare with the “Arts” category.	www.eonline.com www.ew.com
Extreme	extr	1075	Material of a sexually violent or criminal nature; violence and violent behavior; tasteless, often gory photographs, such as autopsy photos; photos of crime scenes, crime and accident victims; excessive obscene material; shock websites.	www.car-accidents.com www.crime-scene-photos.com
Fashion	fash	1076	Clothing and fashion; hair salons; cosmetics; accessories; jewelry; perfume; pictures and text relating to body modification; tattoos and piercing; modeling agencies. Dermatological products are classified as “Health and Nutrition.”	www.fashion.net www.findabeautysalon.com

URL Category	Abbreviation	Code	Description	Example URLs
File Transfer Services	fts	1071	File transfer services with the primary purpose of providing download services and hosted file sharing	www.rapidshare.com www.yousendit.com
Filter Avoidance	filt	1025	Promoting and aiding undetectable and anonymous web usage, including cgi, php and glype anonymous proxy services.	www.bypassschoolfilter.com www.filterbypass.com
Finance	fnnc	1015	Primarily financial in nature, such as accounting practices and accountants, taxation, taxes, banking, insurance, investing, the national economy, personal finance involving insurance of all types, credit cards, retirement and estate planning, loans, mortgages. Stock and shares are classified as “Online Trading.”	finance.yahoo.com www.bankofamerica.com
Freeware and Shareware	free	1068	Providing downloads of free and shareware software.	www.freewarehome.com www.shareware.com
Gambling	gamb	1049	Casinos and online gambling; bookmakers and odds; gambling advice; competitive racing in a gambling context; sports booking; sports gambling; services for spread betting on stocks and shares. Websites dealing with gambling addiction are classified as “Health and Nutrition.” Government-run lotteries are classified as “Lotteries”.	www.888.com www.gambling.com
Games	game	1007	Various card games, board games, word games, and video games; combat games; sports games; downloadable games; game reviews; cheat sheets; computer games and Internet games, such as role-playing games.	www.games.com www.shockwave.com
Government and Law	gov	1011	Government websites; foreign relations; news and information relating to government and elections; information relating to the field of law, such as attorneys, law firms, law publications, legal reference material, courts, dockets, and legal associations; legislation and court decisions; civil rights issues; immigration; patents and copyrights; information relating to law enforcement and correctional systems; crime reporting, law enforcement, and crime statistics; military, such as the armed forces, military bases, military organizations; anti-terrorism.	www.usa.gov www.law.com
Hacking	hack	1050	Discussing ways to bypass the security of websites, software, and computers.	www.hackthissite.org www.gohacking.com
Hate Speech	hate	1016	Websites promoting hatred, intolerance, or discrimination on the basis of social group, color, religion, sexual orientation, disability, class, ethnicity, nationality, age, gender, gender identity; sites promoting racism; sexism; racist theology; hate music; neo-Nazi organizations; supremacism; Holocaust denial.	www.kkk.com www.nazi.org

URL Category Descriptions

URL Category	Abbreviation	Code	Description	Example URLs
Health and Nutrition	hlth	1009	Health care; diseases and disabilities; medical care; hospitals; doctors; medicinal drugs; mental health; psychiatry; pharmacology; exercise and fitness; physical disabilities; vitamins and supplements; sex in the context of health (disease and health care); tobacco use, alcohol use, drug use, and gambling in the context of health (disease and health care); food in general; food and beverage; cooking and recipes; food and nutrition, health, and dieting; cooking, including recipe and culinary websites; alternative medicine.	www.health.com www.webmd.com
Humor	lol	1079	Jokes, sketches, comics and other humorous content. Adult humor likely to offend is classified as “Adult.”	www.humor.com www.jokes.com
Illegal Activities	ilac	1022	Promoting crime, such as stealing, fraud, illegally accessing telephone networks; computer viruses; terrorism, bombs, and anarchy; websites depicting murder and suicide as well as explaining ways to commit them.	www.ekran.no www.thedisease.net
Illegal Downloads	ildl	1084	Providing the ability to download software or other materials, serial numbers, key generators, and tools for bypassing software protection in violation of copyright agreements. Torrents are classified as “Peer File Transfer.”	www.keygenguru.com www.zcrack.com
Illegal Drugs	drug	1047	Information about recreational drugs, drug paraphernalia, drug purchase and manufacture.	www.cocaine.org www.hightimes.com
Infrastructure and Content Delivery Networks	infr	1018	Content delivery infrastructure and dynamically generated content; websites that cannot be classified more specifically because they are secured or otherwise difficult to classify.	www.akamai.net www.webstat.net
Internet Telephony	voip	1067	Telephonic services using the Internet.	www.evaphone.com www.skype.com
Job Search	job	1004	Career advice; resume writing and interviewing skills; job placement services; job databanks; permanent and temporary employment agencies; employer websites.	www.careerbuilder.com www.monster.com
Lingerie and Swimsuits	ling	1031	Intimate apparel and swimwear, especially when modeled.	www.swimsuits.com www.victoriassecret.com
Lotteries	lotr	1034	Sweepstakes, contests and state-sponsored lotteries.	www.calottery.com www.flalottery.com
Mobile Phones	cell	1070	Short Message Services (SMS); ringtones and mobile phone downloads. Cellular carrier websites are included in the “Business and Industry” category.	www.cbfsm.com www.zedge.net

URL Category	Abbreviation	Code	Description	Example URLs
Nature	natr	1013	Natural resources; ecology and conservation; forests; wilderness; plants; flowers; forest conservation; forest, wilderness, and forestry practices; forest management (reforestation, forest protection, conservation, harvesting, forest health, thinning, and prescribed burning); agricultural practices (agriculture, gardening, horticulture, landscaping, planting, weed control, irrigation, pruning, and harvesting); pollution issues (air quality, hazardous waste, pollution prevention, recycling, waste management, water quality, and the environmental cleanup industry); animals, pets, livestock, and zoology; biology; botany.	www.enature.com www.nature.org
News	news	1058	News; headlines; newspapers; television stations; magazines; weather; ski conditions.	www.cnn.com news.bbc.co.uk
Non-Governmental Organizations	ngo	1087	Non-governmental organizations such as clubs, lobbies, communities, non-profit organizations and labor unions.	www.panda.org www.unions.org
Non-Sexual Nudity	nsn	1060	Nudism and nudity; naturism; nudist camps; artistic nudes.	www.artenuda.com www.naturistsociety.com
Online Communities	comm	1024	Affinity groups; special interest groups; web newsgroups; message boards. Excludes websites classified as “Professional Networking” or “Social Networking.”	www.igda.org www.ieee.org
Online Storage and Backup	osb	1066	Offsite and peer-to-peer storage for backup, sharing, and hosting.	www.adrive.com www.dropbox.com
Online Trading	trad	1028	Online brokerages; websites that enable the user to trade stocks online; information relating to the stock market, stocks, bonds, mutual funds, brokers, stock analysis and commentary, stock screens, stock charts, IPOs, stock splits. Services for spread betting on stocks and shares are classified as “Gambling.” Other financial services are classified as “Finance.”	www.tdameritrade.com www.scottrade.com
Organizational Email	pem	1085	Websites used to access business email (often via Outlook Web Access).	—
Parked Domains	park	1092	Websites that monetize traffic from the domain using paid listings from an ad network, or are owned by “squatters” hoping to sell the domain name for a profit. These also include fake search websites which return paid ad links.	www.domainzaar.com www.parked.com
Peer File Transfer	p2p	1056	Peer-to-peer file request websites. This does not track the file transfers themselves.	www.bittorrent.com www.limewire.com
Personal Sites	pers	1081	Websites about and from private individuals; personal homepage servers; websites with personal contents; personal blogs with no particular theme.	www.karymullis.com www.stallman.org

URL Category Descriptions

URL Category	Abbreviation	Code	Description	Example URLs
Photo Searches and Images	img	1090	Facilitating the storing and searching for, images, photographs, and clip-art.	www.flickr.com www.photobucket.com
Politics	pol	1083	Websites of politicians; political parties; news and information on politics, elections, democracy, and voting.	www.politics.com www.thisnation.com
Pornography	porn	1054	Sexually explicit text or depictions. Includes explicit anime and cartoons; general explicit depictions; other fetish material; explicit chat rooms; sex simulators; strip poker; adult movies; lewd art; web-based explicit email.	www.redtube.com www.youporn.com
Professional Networking	pnet	1089	Social networking for the purpose of career or professional development. See also “Social Networking.”	www.linkedin.com www.europeanpwn.net
Real Estate	rest	1045	Information that would support the search for real estate; office and commercial space; real estate listings, such as rentals, apartments, and homes; house building.	www.realtor.com www.zillow.com
Reference	ref	1017	City and state guides; maps, time; reference sources; dictionaries; libraries.	www.wikipedia.org www.yellowpages.com
Religion	rel	1086	Religious content, information about religions; religious communities.	www.religionfacts.com www.religioustolerance.org
and B2B	saas	1080	Web portals for online business services; online meetings.	www.netsuite.com www.salesforce.com
Safe for Kids	kids	1057	Directed at, and specifically approved for, young children.	kids.discovery.com www.nickjr.com
Science and Technology	sci	1012	Science and technology, such as aerospace, electronics, engineering, mathematics, and other similar subjects; space exploration; meteorology; geography; environment; energy (fossil, nuclear, renewable); communications (telephones, telecommunications).	www.physorg.com www.science.gov
Search Engines and Portals	srch	1020	Search engines and other initial points of access to information on the Internet.	www.bing.com www.google.com
Sex Education	sxed	1052	Factual websites dealing with sex; sexual health; contraception; pregnancy.	www.avert.org www.scarleteen.com
Shopping	shop	1005	Bartering; online purchasing; coupons and free offers; general office supplies; online catalogs; online malls.	www.amazon.com www.shopping.com
Social Networking	snet	1069	Social networking. See also “Professional Networking.”	www.facebook.com www.twitter.com

URL Category	Abbreviation	Code	Description	Example URLs
Social Science	socs	1014	Sciences and history related to society; archaeology; anthropology; cultural studies; history; linguistics; geography; philosophy; psychology; women's studies.	www.archaeology.org www.anthropology.net
Society and Culture	scty	1010	Family and relationships; ethnicity; social organizations; genealogy; seniors; child-care.	www.childcare.gov www.familysearch.org
Software Updates	swup	1053	Websites that host updates for software packages.	www.softwarepatch.com www.versiontracker.com
Sports and Recreation	sprt	1008	All sports, professional and amateur; recreational activities; fishing; fantasy sports; public parks; amusement parks; water parks; theme parks; zoos and aquariums; spas.	www.espn.com www.recreation.gov
Streaming Audio	aud	1073	Real-time streaming audio content including Internet radio and audio feeds.	www.live-radio.net www.shoutcast.com
Streaming Video	vid	1072	Real-time streaming video including Internet television, web casts, and video sharing.	www.hulu.com www.youtube.com
Tobacco	tob	1078	Pro-tobacco websites; tobacco manufacturers; pipes and smoking products (not marketed for illegal drug use). Tobacco addiction is classified as "Health and Nutrition."	www.bat.com www.tobacco.org
Transportation	trns	1044	Personal transportation; information about cars and motorcycles; shopping for new and used cars and motorcycles; car clubs; boats, airplanes, recreational vehicles (RVs), and other similar items. Note, car and motorcycle racing is classified as "Sports and Recreation."	www.cars.com www.motorcycles.com
Travel	trvl	1046	Business and personal travel; travel information; travel resources; travel agents; vacation packages; cruises; lodging and accommodation; travel transportation; flight booking; airfares; car rental; vacation homes.	www.expedia.com www.lonelyplanet.com
Unclassified	—	—	Websites which are not in the Cisco database are recorded as unclassified for reporting purposes. This may include mistyped URLs.	—
Weapons	weap	1036	Information relating to the purchase or use of conventional weapons such as gun sellers, gun auctions, gun classified ads, gun accessories, gun shows, and gun training; general information about guns; other weapons and graphic hunting sites may be included. Government military websites are classified as "Government and Law."	www.coldsteel.com www.gunbroker.com
Web Hosting	whst	1037	Website hosting; bandwidth services.	www.bluehost.com www.godaddy.com

URL Category	Abbreviation	Code	Description	Example URLs
Web Page Translation	tran	1063	Translation of web pages between languages.	babelfish.yahoo.com translate.google.com
Web-Based Email	mail	1038	Public web-based email services. Websites enabling individuals to access their company or organization's email service are classified as "Organizational Email."	mail.yahoo.com www.hotmail.com

Related Topics

- [Managing Updates to the Set of URL Categories, page 9-4](#)
- [Reporting Uncategorized and Misclassified URLs, page 9-3](#)



Create Policies to Control Internet Requests

- [Overview of Policies: Control Intercepted Internet Requests, page 10-1](#)
- [Managing Web Requests Through Policies Best Practices, page 10-2](#)
- [Policies, page 10-2](#)
- [Policy Configuration, page 10-10](#)
- [Block, Allow, or Redirect Transaction Requests, page 10-10](#)
- [Client Applications, page 10-11](#)
- [Limiting Access by Time of Day, page 10-13](#)
- [Remote Users, page 10-17](#)
- [Troubleshooting Policies, page 10-19](#)

Overview of Policies: Control Intercepted Internet Requests

When the user creates a web request the configured Web Security Appliance intercepts the requests and manages the process of which the request travels to get to its final outcome, be that accessing a particular web site, an email or even accessing an online application. In configuring the Web Security Appliance policies are created to define the criteria and actions of requests made by the user.

Policies are the means by which the Web Security Appliance identifies and controls web requests. When a client sends a web request to a server, the Web Proxy receives the request, evaluates it, and determines to which policy it belongs. Actions defined in the policy are then applied to the request.

The Web Security Appliance uses multiple policy types to manage different aspects of web requests. Policy types might fully manage transactions by themselves or pass transactions along to other policy types for additional processing. Policy types can be groups by the functions they perform, such as access, routing, or security.

AsyncOS evaluates transactions based on policies before it evaluates external dependencies to avoid unnecessary external communication from the appliance. For example, if a transaction is blocked based on a policy that blocks uncategorized URLs, the transaction will not also fail based on a DNS error.

Managing Web Requests Through Policies Task Overview

Step	Task List for Managing Web Requests through Policies	Links to Related Topics and Procedures
1	Set up and sequence Authentication Realms	Authentication Realms, page 6-3
2	(For upstream proxies) Create a proxy group.	Creating Proxy Groups for Upstream Proxies, page 3-14
2	(Optional) Create Custom Client Applications	Client Applications, page 10-11
3	(Optional) Create Custom URL Categories	Creating Custom URL Categories, page 10-15
4	Create Identities	Classifying Users and Client Software, page 7-3
5	(Optional) Create time ranges to Limit Access by Time of Day	Limiting Access by Time of Day, page 10-13
6	Create and Order Policies	<ul style="list-style-type: none"> • Creating a Policy, page 10-5 • Policy Order, page 10-5

Managing Web Requests Through Policies Best Practices

- If you want to use Active Directory user objects to manage web requests, do not use primary groups as criteria. Active Directory user objects to not contain the primary group.

Policies

- [Policy Types, page 10-3](#)
- [Policy Order, page 10-5](#)
- [Creating a Policy, page 10-5](#)

Policy Types

Policy Type	Request Type	Description	Link to task
Access	<ul style="list-style-type: none"> HTTP Decrypted HTTPS FTP 	<p>Block, allow or redirect inbound HTTP, FTP, and decrypted HTTPS traffic.</p> <p>Access policies also manage inbound encrypted HTTPS traffic if the HTTPS proxy is disabled.</p>	Creating a Policy, page 10-5
SOCKS	<ul style="list-style-type: none"> SOCKS 	Allow or block SOCKS communication requests.	Creating a Policy, page 10-5
Application Authentication	<ul style="list-style-type: none"> application 	<p>Allow or deny access to a Software as a Service (SaaS) application.</p> <p>Use single sign-on to authenticate users and increase security by allowing access to applications to be quickly disabled.</p> <p>To use the single sign-on feature of policies you must configure the Web Security appliance as an identity provider and upload or generate a certificate and key for SaaS.</p>	Creating SaaS Application Authentication Policies, page 8-4
Encrypted HTTPS Management	<ul style="list-style-type: none"> HTTPS 	<p>Decrypt, pass through, or drop HTTPS connections.</p> <p>AsyncOS passes decrypted traffic to Access policies for further processing.</p>	Creating a Policy, page 10-5
Data Security	<ul style="list-style-type: none"> HTTP Decrypted HTTPS FTP 	Manage data uploads to the web. Data Security policies scan outbound traffic to ensure it complies to company rules for data uploads, based on its destination and content. Unlike External DLP policies, which redirect outbound traffic to external servers for scanning, Data Security policies use the Web Security appliance to scan and evaluate traffic.	Creating a Policy, page 10-5
External DLP (Data Loss Prevention)	<ul style="list-style-type: none"> HTTP Decrypted HTTPS FTP 	Send outbound traffic to servers running 3rd-party DLP systems, which scan it for adherence to company rules for data uploads. Unlike Data Security policies, which also manage data uploads, External DLP policies move scanning work away from the Web Security appliance, which frees resources on the appliance and leverages any additional functionality offered by 3rd-party software.	Creating a Policy, page 10-5

Policy Type	Request Type	Description	Link to task
Outbound Malware Scanning	<ul style="list-style-type: none"> • HTTP • Decrypted HTTPS • FTP 	<p>Block, monitor, or allow requests to upload data that may contain malicious data.</p> <p>Prevent malware that is already present on your network from being transmitted to external networks.</p>	Creating a Policy, page 10-5
Routing	<ul style="list-style-type: none"> • HTTP • HTTPS • FTP 	<p>Direct web traffic through upstream proxies or direct it to destination servers. You might want to redirect traffic through upstream proxies to preserve your existing network design, to off-load processing from the Web Security appliance, or to leverage additional functionality provided by 3rd-party proxy systems.</p> <p>If multiple upstream proxies are available, the Web Security appliance can use load balancing techniques to distribute data to them.</p>	Creating a Policy, page 10-5

Each policy type uses a policy table to store and manage its policies. Each policy table comes with a predefined, global policy, which maintains default actions for a policy type. Additional, user-defined policies are created and added to the policy table as required. Policies are processed in the order in which they are listed in the policy table.

Individual policies define the request types they manage and the actions they perform on those requests. Each policy has two main parts:

1. **Criteria.** The criteria used to identify the requests to which the policy applies. One or more criteria can be specified in a policy and all must be match for the criteria to be met. The criteria are
 - **Protocols.** Allow the transfer of data between various networking devices such as http, https, ftp, etc.
 - **Subnet.** The logical grouping of connected network devices (such as geographic location or Local Area Network [LAN]), where the request originated
 - **Proxy Port.** the numbered port by which the request accesses the web proxy,
 - **Limiting Access by Time of Day.** Time ranges can be created for use in policies to identify or apply actions to web requests based on the time or day the requests were made. The time ranges are created as individual units.
 - **URL Categories.** URL categories are predefined or custom categories of websites, such as News, Business, Social Media, etc. These can be used to identify or apply actions to web requests.
 - **User Agents.** These are the client applications (such as a web browser Firefox or Chrome) used to make requests. You can define policy criteria based on user agents, and you can specify control settings based on user agents. You can also exempt user agents from authentication, which is useful for applications that cannot prompt for credentials. You can define custom client applications but cannot reuse these definitions other policies.

**Note**

When you define multiple membership criteria, the client request must meet all criteria to match the policy.

- 2. Actions.** The actions a policy will apply to requests that match its membership criteria. Actions are typically to block or allow requests, but other actions, such as to scan or redirect requests, are also possible, depending on the policy type.

Criteria must be specified when creating user-defined policies but actions are inherited from global policies until explicitly defined. Most global policies are permissive by default, which means they allow all requests. The SOCKS global policy blocks all traffic by default, however.

Identities. Identities are used in policy membership criteria and are particularly important as they contain many options for identifying web transaction. They also share many properties with policies. Identities are created as individual units.

Policy Order

The order in which policies are listed in a policy table determines the priority with which they are applied to web requests. Web requests are checked against policies beginning at the top of the table and ending at the first policy matched. Any policies below that point in the table are not processed.

If no user-defined policy is matched against a web request, then the global policy for that policy type is applied. Global policies are always positioned last in policy tables and cannot be reordered.

Creating a Policy

Before you begin

- Enable the appropriate proxy:
 - Web Proxy (for HTTP, decrypted HTTPS, and FTP)
 - HTTPS Proxy
 - SOCKS Proxy
- Create associated identities.
- Understand [Policy Order, page 10-5](#).
- (Encrypted HTTPS only) Upload or generate a Certificate and Key.
- (Data Security only) Enable Cisco Data Security Filters Settings.
- (External DLP only) Define an External DLP server.
- (Routing only) Define the associated upstream proxy on the Web Security appliance.
- (Optional) Create associated client applications.
- (Optional) Create associated time ranges in Limiting Access by Time of Day.
- (Optional) Create associated URL categories.

Step 1 From the Web Security Manager menu, select one of these policy types:

- Access
- Encrypted HTTPS
- Data Security
- External DLP
- Outbound Malware Scanning

- Routing
- SOCKS

Step 2 Click **Add Policy**.

Step 3 Assign a name that is unique to the type of policy.

Step 4 (Optional) Enter a description.

Step 5 Considering the desired policy order, using the **Insert Above** field drop-down list, choose where in the policies table to place the policy.

Step 6 In the **Identities and Users** section, choose one or more Identities to which this policy will apply.



Note

HTTPS: If the Identity requires authentication, consider that authentication information may not be available when a user tries to connect to an HTTPS server.

Step 7 (Optional) Expand the **Advanced** section to apply this policy to transactions based on additional transaction characteristics.

Advanced Option	Description
Protocols	Select the protocols to which this policy will apply. “All others” means any protocol not listed above this option. If the associated identity applies to specific protocols, this policy applies to those same protocols...
Proxy Ports	Apply this policy only to traffic using specific ports to access the web proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas. For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. Note If the associated identity applies only to specific proxy ports, the web interface will not allow you to enter proxy ports here.
Subnets	Apply this policy only to traffic on specific subnets. Note If the associated identity applies to specific subnets, you can further restrict the application of this policy to a subset of the addresses to which the identity applies.
Limiting Access by Time of Day	Apply this policy only to traffic on specific subnets.
URL Categories	Apply this policy only to traffic on specific subnets. Note If the associated identity applies to specific subnets, you can further restrict the application of this policy to a subset of the addresses to which the identity applies.
Client Applications	Apply this policy only to traffic on specific subnets. Note If the associated identity applies to specific subnets, you can further restrict the application of this policy to a subset of the addresses to which the identity applies.

Step 8 Configure the policy to manage web requests:

- a. Review the actions available to apply to specific types of content.

Action	Description
Use Global Setting	Uses the action for this category in the Global Policy. This is the default action for user defined policies. Applies to user defined policies only.
Block	The Web Proxy stops transactions that match this setting.
Redirect	Redirects traffic originally destined for a URL in this category to a location you specify. When you choose this action, the Redirect To field appears. Enter a URL to which to redirect all traffic.
Allow	Always allows client requests for web sites in this category. Allowed requests bypass all further filtering and malware scanning.
Monitor	The Web Proxy neither allows nor blocks the request. Instead, it continues to evaluate the client request against other policy group control settings, such as web reputation filtering.
Warn	The Web Proxy initially blocks the request and displays a warning page, but allows the user to continue by clicking a hypertext link in the warning page.
Time-Based	The Web Proxy blocks or monitors the request during the time ranges you specify.

- b. Specify the action to take for each type of content.

- (Optional) Apply specific actions to requests for Protocols and Client Applications:


Option	Additional Steps
Use Global Policy Setting	—
Define Custom Settings	<ol style="list-style-type: none"> Click to Block FTP over HTTP, HTTP or Native FTP Define HTTP Connect Ports (enables applications to tunnel outbound traffic over HTTP). Leave blank to block all ports. Block Custom Client Applications (for example; Firefox, MSN, Skype)
Disable Settings for this Policy	Do not use protocol, HTTP connection ports, or client application to block requests.

- (Optional) Apply specific actions to requests for URL Categories:

Option	Additional Steps
Custom URL Category Filtering	<ol style="list-style-type: none"> Click Select Custom Categories. Choose which custom URL categories to include/exclude in this policy and click Apply. Select the action to apply to the included categories. Submit.
Predefined URL Category Filtering	<ol style="list-style-type: none"> Select the action to apply to the predefined URL categories. Submit.

Option	Additional Steps
Uncategorized URLs	<ol style="list-style-type: none"> 1. Select the action to apply to uncategorized URLs. 2. Select the action to apply to the update categories. 3. Submit.
Content Filtering	<ol style="list-style-type: none"> 1. Choose Define Content Filtering Custom Settings from the drop-down menu 2. (Optional) Click the Enable Safe Search check box. 3. Choose whether to block users from search engines that are not currently supported by the Web Security appliance safe search feature. 4. (Optional) Click the Enable Site Content Rating check box. 5. Choose whether to block all adult content from the supported content ratings websites or to display the end-user URL filtering warning page.

- (Optional) Apply an action to requests to connect with specific Applications:

Option	Additional Steps
Click the  button beside the application	<ol style="list-style-type: none"> 1. Select the link of the required application 2. Set the action for that application <ul style="list-style-type: none"> • Use Global Setting (Monitor) • Monitor • Monitor and Block Posting Text • Block
Select the Edit all... option	<ol style="list-style-type: none"> 1. Set the action for that application <ul style="list-style-type: none"> • Leave current settings • Use Global Setting (Monitor) • Block • Monitor 2. Click Apply

- (Optional) Block objects based on size or type:

Option	Additional Steps
Use Global Policy Setting	—
Define Custom Object Blocking Settings	<ol style="list-style-type: none"> 1. Define object size for: <ul style="list-style-type: none"> • HTTP/HTTPS Max Download Size • FTP Max Download Size. 2. Select Object Type to Block from the predefined list. 3. Block Custom MIME types (for example; WAV, MP4, WMV)
Disable Object Blocking for this Policy	Do not block objects

- (Optional) Manage suspected malware:

Option	Additional Steps
Web Reputation Settings	1. Check to enable Web Reputation Filtering
DVS Anti-Malware settings	1. Enable Suspect Client Applications Scanning 2. Enable Anti-Malware Scanning (Webroot, McAfee and Sophos) 3. Select whether to monitor or block each malware category

Step 9 Submit and Commit Changes.

Related Topics

- [Creating a Time Range](#)
 - [Using Client Applications in Policies](#)
-

Policy Configuration

Option	Description
Protocols and Client Applications	Used to control policy access to protocols and configure blocking for particular client applications, such as instant messaging clients, web browsers, and Internet phone services. You can also configure the appliance to tunnel HTTP CONNECT requests on specific ports. With tunneling enabled, the appliance passes HTTP traffic through specified ports without evaluating it.
URL Categories	AsyncOS for Web allows you to configure how the appliance handles a transaction based on the URL category of a particular HTTP or HTTPS request. Using a predefined category list, you can choose to monitor, block, warn or set time-based content by category. You can also create custom URL categories and choose to allow, monitor, block, warn, redirect or configure time-based traffic for a website in the custom category.
Applications	The Application Visibility and Control engine (AVC engine) is an acceptable use policy component that inspects web traffic to gain deeper understanding and control of web traffic used for applications. The appliance allows the Web Proxy to be configured to block or allow applications by application type or a particular application. You can also apply controls to particular application behaviors within a particular application, such as file transfers.
Object Blocking	<p>Allows the Web Proxy to be configured to block file downloads based on file characteristics, such as file size and file type. An object is, generally, any item that can be individually selected, uploaded, downloaded and manipulated, such as:</p> <ul style="list-style-type: none"> • Application: pdf, xml, zip, exe • Text: cmd, csv, html, javascript • Image: gif, jpeg, png, tiff • Video: mp4, Quicktime, avi, wmv • Audio: mp4, wav, webm, mpeg • Message: http, xml, rfc822, partial • x-world: wrl, wrz, xof, 3dmf <p>Note Object blocking does not inspect inside compressed files.</p>
Anti-Malware and Reputation	<p>Web reputation filters allow for a web-based reputation score to be assigned to a URL to determine the probability of it containing URL-based malware. Anti-malware scanning identifies and stops web-based malware threats. Advanced Malware Protection identifies malware in downloaded files.</p> <p>The Anti-Malware and Reputation policy inherits global settings respective to each component. Within Security Services > Anti-Malware and Reputation, malware categories can be customized to monitor or block based on malware scanning verdicts and web reputation score thresholds can be customized. Malware categories can be further customized within a policy. There are also global settings for file reputation and analysis services.</p> <p>For more information, see Web Reputation and Anti-Malware Anti-Malware and Reputation Settings in Access Policies, page 13-11 and Enable File Reputation Evaluation Per Access Policy, page 28-5.</p>

Block, Allow, or Redirect Transaction Requests

The web proxy controls web traffic based on the policies that you create for groups of transaction requests.

- **Allow.** The Web Proxy permits the connection without interruption. Allowed connections may not have been scanned by the DVS engine.
- **Block.** The Web Proxy does not permit the connection and instead displays an end user notification page explaining the reason for the block.
- **Redirect.** The Web Proxy does not allow the connection to the originally requested destination server and instead connects to a different specified URL, see [Redirecting Traffic in the Access Policies](#).



Note

The preceding actions are final actions that the Web Proxy takes on a client request. The Monitor action that you can configure for Access Policies is not a final action.

Generally, different types of policies control traffic based on the transport protocol.

Policy Type	Protocols				Actions Supported			
	HTTP	HTTPS	FTP	SOCKS	Block	Allow	Redirect	Monitor
Access	x	x	x		x	x	x	x
SOCKS				x	x	x		
SAAS	x	x						
Decryption	x	x						x
Data Security	x	x	x		x			x
External DLP	x	x	x				x	
Outbound Malware Scanning	x	x	x		x			x
Routing	x	x	x				x	



Note

Decryption policy takes precedence over Access policy.

Client Applications

About Client Applications

Client Applications (such as a web browser) are used to make requests. You can define policy membership based on client applications, and you can specify control settings and exempt client applications from authentication, which is useful for applications that cannot prompt for credentials.

Using Client Applications in Policies

Defining Policy Membership Using Client Applications

- Step 1** Choose a policy type from the Web Security Manager menu.
- Step 2** Click a policy name in the policies table.
- Step 3** Expand the Advanced section and click the link in the Client Applications field.
- Step 4** Define one or more of the client applications:

Table 10-1

Option	Method
Choose a predefined client application	Expand the Browser and Other sections and check the required client application check boxes. Tip Choose only the Any Version options when possible, as this provides better performance than having multiple selections.
Define a custom client application	Enter an appropriate regular expression in the Custom Client Applications field. Enter additional regular expressions on new lines as required. Tip Click Example Client Applications Patterns for examples of regular expressions.

- Step 5** (Optional) Click the **Match All Except The Selected Client Applications Definitions** radio button to base the policy membership on all client applications **except** those you have defined.
- Step 6** Click **Done**.

Defining Policy Control Settings Using Client Applications

- Step 1** Choose a policy type from the Web Security Manager menu.
- Step 2** Find the required policy name in the policies table.
- Step 3** Click the cell link in the Protocols and Client Applications column on the same row.
- Step 4** Choose **Define Custom Settings** from the drop-down list in the Edit Protocols and Client Applications Settings pane (if not already set).
- Step 5** Enter a regular expression in the Custom Client Applications field that matches the client application you wish to define. Enter additional regular expressions on new lines as required.



Tip Click **Example Client Application Patterns** for examples of regular expressions.

- Step 6** Submit and commit your changes.

Exempting Client Applications from Authentication

Step	Task	Link
Step 1	Create an Identity that does not require authentication.	Classifying Users and Client Software
Step 2	Set the Identity membership as the client application to exempt.	Using Client Applications in Policies
Step 3	Place the Identity above all other Identities in the policies table that require authentication.	Policy Order

Limiting Access by Time of Day

About Limiting Access by Time of Day

A defined time range can limit the times at which Routing, Access, Encrypted HTTPS Management, and SOCKS policies are enforced. They can be used to define policy membership, which limits the time the entire policy is enforced. They can also be used to define URL filtering control settings, which limits the time that this control is applied.



Note

You cannot use time ranges to define the times at which users must authenticate. Authentication requirements are defined in Identities, which do not support time ranges.

Creating a Time Range

- Step 1** Choose **Web Security Manager > Defined Time Ranges**.
- Step 2** Click **Add Time Range**.
- Step 3** Enter a name for the time range.
- Step 4** Choose a Time Zone option:

Table 10-2

Option	Description
Use Time Zone Setting From Appliance	Use the same time zone as the Web Security appliance.
Specify Time Zone For Limiting Access by Time of Day	Configure a time zone which is different to that used by the Web Security appliance.

- Step 5** Check one or more Day of Week check boxes.

Step 6 Choose a Time Of Day option:

Table 10-3

Option	Description
All Day	Use the full 24-hour period.
From / To	Define a specific hourly range. Enter a start and end time in HH:MM (24 hour format).



Tip

Each time range includes the start time and excludes the end time. For example, entering 8:00 through 17:00 matches 8:00:00 through 16:59:59, but not 17:00:00. Midnight must be specified as 00:00 for a start time, and as 24:00 for an end time.

Step 7 (Optional) Click **Add Row** and repeat steps 5 and 6 to define another Day of Week and Time of Day combination.

Step 8 Submit and commit your changes.

Using Limiting Access by Time of Day in Policies

Step 1 Choose a policy type from the Web Security Manager menu.

Step 2 Click a policy name in the policies table.

Step 3 Expand the **Advanced** section and click the link in the Limiting Access by Time of Day field.

Step 4 Choose the time range you wish to use in the Limiting Access by Time of Day drop-down list.

Step 5 Click the **Match Except During The Selected Limiting Access by Time of Day** radio button to have the policy match times outside the time range you have specified.

Step 6 Submit and commit your changes.

Controlling Access by URL Category

About Controlling Access by URL Category

You can identify and action web requests based on the category of website they address. The Web Security appliance ships with many predefined URL categories by default, such as Web-based Email and others.

Predefined categories, and the websites associated with them, are defined within filtering databases that reside on the Web Security appliance. These databases are automatically kept up to date by Cisco. You can also create user-defined custom URL categories, however, for hostnames and IP addresses that you specify.

URL categories can be used by all policies except policies to identify requests. They can also be used by Access, Encrypted HTTPS Management and Data Security policies to apply actions to requests.

Before you can use create or use URL categories you must enable Acceptable Use Control on the Web Security appliance.

Creating Custom URL Categories

Before you begin

- Enable Acceptable Use Control, see [Configuring the URL Filtering Engine](#).

Step 1 Choose **Web Security Manager > Custom URL Categories**.

Step 2 Click **Add Custom Category**.

Step 3 Enter the settings for the custom URL category:

Table 10-4

Setting	Description
Category Name	Enter a name for the URL category. This name appears when you configure URL filtering for policies. Note: The Sawmill for reporting tool will not find custom URL categories in access logs if their names contain spaces in the first four characters.
List Order	Choose the order in the list of custom URL categories to place this category. Enter “1” for the topmost URL category. The URL filtering engine evaluates a client request against the custom URL categories in the order specified.
Sites	Enter one or more addresses that belong in the custom category. You can enter multiple addresses separated by line breaks or commas. You can enter addresses using any of the following formats: <ul style="list-style-type: none"> • IP address, such as 10.1.1.0 • CIDR address, such as 10.1.1.0/24 • Domain name, such as example.com • Hostname, such as crm.example.com • Partial hostname, such as .example.com Note: Entering a partial hostname, such as .example.com, also matches www.example.com. Note: It is possible to use the same address in multiple custom URL categories, but the order in which the categories are listed in is relevant. If you include these categories in the same policy, and define different actions to each one, then the action of the category listed highest in the custom URL categories table is what takes effect.
Advanced: Regular Expressions	You can use regular expressions to specify multiple web servers that match the pattern you enter. Note: The URL filtering engine compares URLs with addresses entered in the Sites field first. If the URL of a transaction matches an entry in the Sites field, it is not compared to any expression entered here.

Step 4 (Optional) Click **Sort URLs** to sort all addresses in the Sites field into alphanumeric order.



Note Once you sort the addresses, you cannot retrieve their original order.

Step 5 Submit and commit your changes.

Related Topics

- [Regular Expressions](#)

Using URL Categories to Identify Web Requests

Before You Begin

- Enable Acceptable Use Control, see [Configuring the URL Filtering Engine](#).
 - (Optional) Create Custom URL Categories, see [Creating Custom URL Categories](#).
-

- Step 1** Choose a policy type (except SaaS) from the Web Security Manager menu.
- Step 2** Click a policy name in the policies table (or add a new policy).
- Step 3** Expand the **Advanced** section and click the link in the URL Categories field.
- Step 4** Click the Add column cells corresponding to URL Categories you wish to identify web requests by. Do this for the Custom URL Categories and Predefined URL Categories lists as required.
- Step 5** Click **Done**.
- Step 6** Submit and commit your changes.
-

Using URL Categories to Action Web Request

Before you begin

- Enable Acceptable Use Control, see [Configuring the URL Filtering Engine](#).
- (Optional) Create Custom URL Categories, see [Creating Custom URL Categories](#).



Note If you have used URL categories as criteria within a policy then those categories alone are available to specify actions against within the same policy. Some of the options described below may differ or be unavailable because of this.

- Step 1** Choose one of **Access Policies**, **Cisco Data Security Policies**, or **Encrypted HTTPS Management** from the Web Security Manager menu.
- Step 2** Find the required policy name in the policies table.
- Step 3** Click the cell link in the URL Filtering column on the same row.
- Step 4** (Optional) Add custom URL categories:
- Click **Select Custom Categories**.
 - Choose which custom URL categories to include in this policy and click **Apply**.

Choose which custom URL categories the URL filtering engine should compare the client request against. The URL filtering engine compares client requests against included custom URL categories, and ignores excluded custom URL categories. The URL filtering engine compares the URL in a client request to included custom URL categories before predefined URL categories.

The custom URL categories included in the policy appear in the Custom URL Category Filtering section.

Step 5 Choose an action for each custom and predefined URL category.



Note Available actions vary between custom and predefined categories and between policy types.

Step 6 In the Uncategorized URLs section, choose the action to take for client requests to web sites that do not fall into a predefined or custom URL category.

Step 7 Submit and commit your changes.

Remote Users

- [About Remote Users, page 10-17](#)
- [Configuring Identification for Remote Users, page 10-18](#)
- [Display Remote User Status and Statistics for ASAs, page 10-19](#)

About Remote Users

Cisco AnyConnect Secure Mobility extends the network perimeter to remote endpoints, enabling the integration of web filtering services offered by the Web Security appliance.

Remote and mobile users use the Cisco AnyConnect Secure VPN (virtual private network) client to establish VPN sessions with the Adaptive Security Appliance (ASA). The ASA sends web traffic to the Web Security appliance along with information identifying the user by IP address and user name. The Web Security appliance scans the traffic, enforces acceptable use policies, and protects the user from security threats. The security appliance returns all traffic deemed safe and acceptable to the user.

When Secure Mobility is enabled, you can configure identities and policies to apply to users by their location:

- **Remote users.** These users are connected to the network from a remote location using VPN. The Web Security appliance automatically identifies remote users when both the Cisco ASA and Cisco AnyConnect client are used for VPN access. Otherwise, the Web Security appliance administrator must specify remote users by configuring a range of IP addresses.
- **Local users.** These users are connected to the network either physically or wirelessly.

When the Web Security appliance integrates with a Cisco ASA, you can configure it to identify users by an authenticated user name transparently to achieve single sign-on for remote users.

Configuring Identification for Remote Users

Task	Further information
1. Configure identification of remote users.	Configuring Identification of Remote Users, page 10-18
2. Create an identity for remote users.	Classifying Users and Client Software, page 7-3 <ol style="list-style-type: none"> In the “Define Members by User Location” section, select Remote Users Only. In the “Define Members by Authentication” section, select “Identify Users Transparently through Cisco ASA Integration.”
3. Create a policy for remote users.	Creating a Policy, page 10-5

Configuring Identification of Remote Users

- Step 1** Security Services > AnyConnect Secure Mobility, and click **Enable**.
- Step 2** Read the terms of the AnyConnect Secure Mobility License Agreement, and click **Accept**.
- Step 3** Configure how to identify remote users.

Option	Description	Additional Steps
IP Address	Specify a range of IP addresses that the appliance should consider as assigned to remote devices.	<ol style="list-style-type: none"> Enter a range of IP addresses in the IP Range field. Go to step 4
Cisco ASA Integration	Specify one or more Cisco ASA the Web Security appliance communicates with. The Cisco ASA maintains an IP address-to-user mapping and communicates that information with the Web Security appliance. When the Web Proxy receives a transaction, it obtains the IP address and determines the user by checking the IP address-to-user mapping. When users are determined by integrating with a Cisco ASA, you can enable single sign-on for remote users.	<ol style="list-style-type: none"> Enter the Cisco ASA host name or IP address. Enter the port number used to access the ASA. The default port number for the Cisco ASA is 11999. If multiple Cisco ASA are configured in a cluster, click Add Row and configure each ASA in the cluster. <p>Note If two Cisco ASA are configured for high availability, enter only one host name or IP address for the <i>active</i> Cisco ASA.</p> <ol style="list-style-type: none"> Enter the access password for the Cisco ASA. <p>Note The password you enter here must match the access password configured for the specified Cisco ASA.</p> <ol style="list-style-type: none"> Optional, click Start Test to verify the Web Security appliance can connect to the configured Cisco ASA.

Step 4 Submit and Commit Changes.

Display Remote User Status and Statistics for ASAs

Use this command to display information related to Secure Mobility when the Web Security appliance is integrated with an ASA.

Command	Description
<code>musstatus</code>	<p>This command displays the following information:</p> <ul style="list-style-type: none"> • The status of the Web Security appliance connection with each ASA. • The duration of the Web Security appliance connection with each ASA in minutes. • The number of remote clients from each ASA. • The number of remote clients being serviced, which is defined as the number of remote clients that have passed traffic through the Web Security appliance. • The total number of remote clients.

Troubleshooting Policies

- [Access Policy not Configurable for HTTPS, page A-7](#)
- [Some Microsoft Office Files Not Blocked, page A-8](#)
- [Blocking DOS Executable Object Types Blocks Updates for Windows OneCare, page A-8](#)
- [Identity Disappeared from Policy, page A-8](#)
- [Policy is Never Applied, page A-8](#)
- [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, page A-9](#)
- [User Matches Global Policy for HTTPS and FTP over HTTP Requests, page A-9](#)
- [User Assigned Incorrect Access Policy, page A-9](#)
- [Policy Troubleshooting Tool: Policy Trace, page A-10](#)



Create Decryption Policies to Control HTTPS Traffic

- [Overview of Create Decryption Policies to Control HTTP Traffic, page 11-1](#)
- [Managing HTTPS Traffic through Decryption Policies Best Practices, page 11-2](#)
- [Decryption Policies, page 11-2](#)
- [Certificates, page 11-5](#)
- [Routing HTTPS Traffic, page 11-11](#)

Overview of Create Decryption Policies to Control HTTP Traffic

Decryption policies define the handling of HTTPS traffic within the web proxy:

- When to decrypt HTTPS traffic.
- How to handle requests that use invalid or revoked security certificates.

You can create decryption policies to handle HTTPS traffic in the following ways:

- Pass through encrypted traffic
- Decrypt traffic and apply the content-based access policies defined for HTTP traffic. This also makes malware scanning possible.
- Drop the HTTPS connection
- Monitor the request (take no final action) as the web proxy continues to evaluate the request against policies that may lead to a final drop, pass through, or decrypt action.



Caution

Handle personally identifiable information with care: If you choose to decrypt an end-user's HTTPS session, the Web Security appliance access logs and reports may contain personally identifiable information. The Administrator can configure how much URI text is stored in the logs using the `advancedproxyconfig` CLI command and the `HTTPS` subcommand. You can log the entire URI, or a partial form of the URI with the query portion removed. However, even when you choose to strip the query from the URI, personally identifiable information may still remain.

Managing HTTPS Traffic through Decryption Policies Task Overview

Step	Task List for Managing HTTPS Traffic through Decryption Policies	Links to Related Topics and Procedures
1	Enabling the HTTPS proxy	Enabling the HTTPS Proxy, page 11-3
2	Upload or Generate a certificate and key	<ul style="list-style-type: none"> • Uploading a Root Certificate and Key, page 11-7 • Generating a Certificate and Key, page 11-8
3	Configuring Decryption options	Configuring Decryption Options, page 11-4
5	(Optional) Configure invalid certificate handling	Configuring Invalid Certificate Handling, page 11-8
6	(Optional) Enabling real-time revocation status checking	Enabling Real-Time Revocation Status Checking, page 11-10
7	(Optional) Manage trusted and blocked certificates	Trusted Root Certificates, page 11-10

Managing HTTPS Traffic through Decryption Policies Best Practices

- Create fewer, more general Decryption Policy groups that apply to all users or fewer, larger groups of users on the network. Then, if you need to apply more granular control to decrypted HTTPS traffic, use more specific Access Policy groups.

Decryption Policies

The appliance can perform any of the following actions on an HTTPS connection request:

Option	Description
Monitor	Monitor is an intermediary action that indicates the Web Proxy should continue evaluating the transaction against the other control settings to determine which final action to ultimately apply.
Drop	The appliance drops the connection and does not pass the connection request to the server. The appliance does not notify the user that it dropped the connection.
Pass through	The appliance passes through the connection between the client and the server without inspecting the traffic content.
Decrypt	The appliance allows the connection, but inspects the traffic content. It decrypts the traffic and applies Access Policies to the decrypted traffic as if it were a plaintext HTTP connection. By decrypting the connection and applying Access Policies, you can scan the traffic for malware.

Enabling the HTTPS Proxy

To monitor and decrypt HTTPS traffic, you must enable the HTTPS Proxy. When you enable the HTTPS Proxy, you must configure what the appliance uses for a root certificate when it sends self-signed server certificates to the client applications on the network. You can upload a root certificate and key that your organization already has, or you can configure the appliance to generate a certificate and key with information you enter.

Once the HTTPS Proxy is enabled, all HTTPS policy decisions are handled by Decryption Policies. Also on this page, you can configure what the appliance does with HTTPS traffic when the server certificate is invalid.

Before You Begin

- When the HTTPS proxy is enabled, HTTPS-specific rules in access policies are disabled and the web proxy processes decrypted HTTPS traffic using rules for HTTP.

Step 1 Security Services > HTTPS Proxy, click **Enable and Edit Settings**.

The HTTPS Proxy License Agreement appears.

Step 2 Read the terms of the HTTPS Proxy License Agreement, and click **Accept**.

Step 3 Verify the Enable HTTPS Proxy field is enabled.

Step 4 In the HTTPS Ports to Proxy field, enter the ports the appliance should check for HTTPS traffic. Port 443 is the default port.



Note

The maximum number of ports for which the Web Security appliance can serve as proxy is 30, which includes both HTTP and HTTPS.

Step 5 Upload **or** generate a root/signing certificate to use for decryption.



Note

If the appliance has both an uploaded certificate and key pair and a generated certificate and key pair, it only uses the certificate and key pair currently selected in the Root Certificate for Signing section.

Step 6 In the HTTPS Transparent Request section, select one of the following options:

- Decrypt the HTTPS request and redirect for authentication
- Deny the HTTPS request

This setting only applies to transactions that use IP address as the authentication surrogate and when the user has not yet been authenticated.



Note

This field only appears when the appliance is deployed in transparent mode.

Step 7 In the Applications that Use HTTPS section, choose whether to enable decryption for enhanced application visibility and control.



Note

Decryption may cause some applications to fail unless the root certificate for signing is installed on the client. For more information on the appliance root certificate, see.

Step 8 Submit and commit your changes.

Related topics

- [Managing Certificate Validation and Decryption for HTTPS, page 11-6](#)

Controlling HTTPS Traffic

After the Web Security appliance assigns an HTTPS connection request to a Decryption Policy group, the connection request inherits the control settings of that policy group. The control settings of the Decryption Policy group determine whether the appliance decrypts, drops, or passes through the connection:

Option	Description
URL Categories	<p>You can configure the action to take on HTTPS requests for each predefined and custom URL category. Click the link under the URL Categories column for the policy group you want to configure.</p> <p>Note If you want to <i>block</i> (with end-user notification) a particular URL category for HTTPS requests instead of drop (with no end-user notification), choose to decrypt that URL category in the Decryption Policy group and then choose to block the same URL category in the Access Policy group.</p>
Web Reputation	<p>You can configure the action to take on HTTPS requests based on the web reputation score of the requested server. Click the link under the Web Reputation column for the policy group you want to configure.</p>
Default Action	<p>You can configure the action the appliance should take when none of the other settings apply. Click the link under the Default Action column for the policy group you want to configure.</p> <p>Note The configured default action only affects the transaction when no decision is made based on URL category or Web Reputation score. If Web Reputation filtering is disabled, the default action applies to all transactions that match a Monitor action in a URL category. If Web Reputation filtering is enabled, the default action is used only if the Monitor action is selected for sites with no score.</p>

Configuring Decryption Options

Before you begin

- Verify that the HTTPS proxy is enabled as described in [Enabling the HTTPS Proxy, page 11-3](#)
-

Step 1 Security Services > HTTPS Proxy.

Step 2 Click **Edit Settings**.

Step 3 Enable the decryption options.

Decryption Option	Description
Decrypt for Authentication	For users who have not been authenticated prior to this HTTPS transaction, allow decryption for authentication.
Decrypt for End-User Notification	Allow decryption so that AsyncOS can display the end-user notification. Note If the certificate is invalid and invalid certificates are set to drop, when running a policy trace, the first logged action for the transaction will be “decrypt”.
Decrypt for End-User Acknowledgement	For users who have not acknowledged the web proxy prior to this HTTPS transaction, allow decryption so that AsyncOS can display the end-user acknowledgement.
Decrypt for Application Detection	Enhances the ability of AsyncOS to detect HTTPS applications.

Authentication and HTTPS Connections

Authentication at the HTTPS connection layer is available for these types of requests:

Option	Description
Explicit requests	<ul style="list-style-type: none"> secure client authentication disabled or secure client authentication enabled and an IP-based surrogate
Transparent requests	<ul style="list-style-type: none"> IP-based surrogate, decryption for authentication enabled or IP-based surrogate, client previously authenticated using an HTTP request

Certificates

The HTTPS proxy uses the root certificates and private key files that you upload to the appliance to decrypt traffic. The root certificate and private key files you upload to the appliance must be in PEM format; DER format is not supported.

You can enter root certificate information in the following ways:

- **Generate.** You can enter some basic organization information and then click a button so the appliance generates the rest of the certificate and a private key.
- **Upload.** You can upload a certificate file and its matching private key file created outside of the appliance.

**Note**

You can also upload an intermediate certificate that has been signed by a root certificate authority. When the Web Proxy mimics the server certificate, it sends the uploaded certificate along with the mimicked certificate to the client application. That way, as long as the intermediate certificate is signed by a root certificate authority that the client application trusts, the application will trust the mimicked server certificate, too.

You can choose how to handle the root certificates issued by the Web Security appliance:

- **Inform users to accept the root certificate.** You can inform the users in your organization what the new policies are at the company and tell them to accept the root certificate supplied by the organization as a trusted source.
- **Add the root certificate to client machines.** You can add the root certificate to all client machines on the network as a trusted root certificate authority. This way, the client applications automatically accept transactions with the root certificate.

Step 1 Security Services > HTTPS Proxy.

Step 2 Click **Edit Settings**.

Step 3 Click the Download Certificate link for either the generated or uploaded certificate.

**Note**

To reduce the possibility of client machines getting a certificate error, submit the changes after you generate or upload the root certificate to the Web Security appliance, then distribute the certificate to client machines, and then commit the changes to the appliance.

Managing Certificate Validation and Decryption for HTTPS

The Web Security appliance validates certificates before inspecting and decrypting content.

Valid Certificates

Qualities of a valid certificate:

- **Not expired.** The certificate's validity period includes the current date.
- **Recognized certificate authority.** The issuing certificate authority is included in the list of trusted certificate authorities stored on the Web Security appliance.
- **Valid signature.** The digital signature was properly implemented based on cryptographic standards.
- **Consistent naming.** The common name matches the hostname specified in the HTTP header.
- **Not revoked.** The issuing certificate authority has not revoked the certificate.

Related Topics

- [Managing Certificate Validation and Decryption for HTTPS, page 11-6](#)
- [Configuring Invalid Certificate Handling, page 11-8](#)
- [Options for Certificate Revocation Status Checking, page 11-9](#)

- [Enabling Real-Time Revocation Status Checking, page 11-10](#)

Invalid Certificate Handling

The appliance can perform one of the following actions for invalid server certificates:

- **Drop.**
- **Decrypt.**
- **Monitor.**

Certificates that are Invalid for Multiple Reasons

For server certificates that are invalid due to both an unrecognized root authority and an expired certificate, the HTTPS proxy performs the action that applies to unrecognized root authorities.

In all other cases, for server certificates that are invalid for multiple reasons simultaneously, the HTTPS Proxy performs actions in order from the most restrictive action to the least restrictive action.

Untrusted Certificate Warnings for Decrypted Connections

When the Web Security appliance encounters an invalid certificate and is configured to decrypt the connection, AsyncOS creates an untrusted certificate that requires the end-user to accept or reject the connection. The common name of the certificate is “Untrusted Certificate Warning.”

Adding this untrusted certificate to the list of trusted certificates will remove the end user’s option to accept or reject the connection.

When AsyncOS generates one of these certificates, it creates a proxy log entry with the text “Signing untrusted key” or “Signing untrusted cert”.

Uploading a Root Certificate and Key

Before you begin

- Enable the HTTPS Proxy. [Enabling the HTTPS Proxy, page 11-3.](#)

Step 1 Security Services > HTTPS Proxy.

Step 2 Click **Edit Settings**.

Step 3 Select **Use Uploaded Certificate and Key**.

Step 4 Click **Browse** for the Certificate field to navigate to the certificate file stored on the local machine.

If the file you upload contains multiple certificates or keys, the Web Proxy uses the first certificate or key in the file.

Step 5 Click **Browse** for the Key field to navigate to the private key file.



Note The key length must be 512, 1024, or 2048 bits.

Step 6 Select **Key is Encrypted** if the key is encrypted.

Step 7 Click **Upload Files** to transfer the certificate and key files to the Web Security appliance.

The uploaded certificate information is displayed on the Edit HTTPS Proxy Settings page.

Step 8 (Optional) Click **Download Certificate** so you can transfer it to the client applications on the network.

Generating a Certificate and Key

Before you begin

- Enable the HTTPS Proxy. [Enabling the HTTPS Proxy, page 11-3](#).
-

- Step 1** **Security Services > HTTPS Proxy.**
- Step 2** Click **Edit Settings**.
- Step 3** Select **Use Generated Certificate and Key**.
- Step 4** Click **Generate New Certificate and Key**.
- Step 5** In the Generate Certificate and Key dialog box, enter the information to display in the root certificate. You can enter any ASCII character except the forward slash (/) in the **Common Name** field.
- Step 6** Click **Generate**.
- Step 7** The generated certificate information is displayed on the Edit HTTPS Proxy Settings page.
- Step 8** (Optional) Click **Download Certificate** so you can transfer it to the client applications on the network.
- Step 9** (Optional) Click the **Download Certificate Signing Request** link, so you can submit the Certificate Signing Request (CSR) to a certificate authority (CA).
- Step 10** (Optional) Upload the signed certificate to the Web Security appliance after receiving it back from the CA. You can do this at anytime after generating the certificate on the appliance.
- Step 11** **Submit** and **Commit Changes**.
-

Configuring Invalid Certificate Handling

Before you begin

- Verify that the HTTPS proxy is enabled as described in [Enabling the HTTPS Proxy, page 11-3](#)
-

- Step 1** **Security Services > HTTPS Proxy.**
- Step 2** Click **Edit Settings**.

Step 3 For each type of certificate error, define the proxy response, **Drop**, **Decrypt** or **Monitor**.

Certificate Error Type	Description
Expired	The current date falls outside of the range of validity for the certificate.
Mismatched hostname	The hostname in the certificate does not match the hostname the client was trying to access. Note The Web Proxy can only perform hostname match when it is deployed in explicit forward mode. When it is deployed in transparent mode, it does not know the hostname of the destination server (it only knows the IP address), so it cannot compare it to the hostname in the server certificate.
Unrecognized root authority/issuer	Either the root authority or an intermediate certificate authority is unrecognized.
Invalid signing certificate	There was a problem with the signing certificate.
Invalid leaf certificate	There was a problem with the leaf certificate, for example, a rejection, decoding, or mismatch problem.
All other error types	Most other error types are due to the appliance not being able to complete the SSL handshake with the HTTPS server. For more information about additional error scenarios for server certificates, see http://www.openssl.org/docs/apps/verify.html .

Step 4 **Submit and Commit Changes.**

Options for Certificate Revocation Status Checking

To determine whether the issuing certificate authority has revoked a certificate, the Web Security appliance can check with the issuing certificate authority in these ways:

- **Certificate Revocation List (Comodo certificates only).** The Web Security appliance checks Comodo's certificate revocation list. Comodo maintains this list, updating it according to their own policies. Depending on when it was last updated, the certificate revocation list may be out of date at the time the Web Security appliance checks it.
- **Online Certificate Status Protocol (OCSP).** The Web Security appliance checks the revocation status with the issuing certificate authority in real time. If the issuing certificate authority supports OCSP, the certificate will include a URL for real-time status checking. This feature is enabled by default for fresh installations and disabled by default for updates.



Note

The Web Security appliance only performs the OCSP query for certificates that it determines to be valid in all other respects and that include the OCSP URL.

Related Topics

- [Enabling Real-Time Revocation Status Checking, page 11-10](#)
- [Configuring Invalid Certificate Handling, page 11-8](#)

Enabling Real-Time Revocation Status Checking

Before you Begin

- Ensure the HTTPS Proxy is enabled. See [Enabling the HTTPS Proxy, page 11-3](#)

Step 1 Security Services > HTTPS Proxy.

Step 2 Click **Edit Settings**.

Step 3 Select **Enable Online Certificate Status Protocol (OCSP)**.

Step 4 Configure the **OCSP Result Handling** properties,

Cisco recommends configuring the OCSP Result Handling options to the same actions as Invalid Certificate Handling options. For example, if you set Expired Certificate to Monitor, configure Revoked Certificate to monitor.

Step 5 (Optional) Expand the Advanced configuration section and configure the settings described below.

Field Name	Description
OCSP Valid Response Cache Timeout	Time to wait before rechecking a valid OCSP response in seconds (s), minutes (m), hours (h), or days (d). Default unit is seconds. Valid range is from 1 second to 7 days.
OCSP Invalid Response Cache Timeout	Time to wait before rechecking an invalid OCSP response in seconds (s), minutes (m), hours (h), or days (d). Default unit is seconds. Valid range is from 1 second to 7 days.
OCSP Network Error Cache Timeout	Time to wait before attempting to contact the OCSP responder again after failing to get a response in seconds (s), minutes (m), hours (h), or days (d). Valid range from 1 second to 24 hours.
Allowed Clock Skew	Maximum allowed difference in time settings between the Web Security appliance and the OCSP responder in seconds (s) or minutes (m). Valid range from 1 second to 60 minutes.
Maximum Time to Wait for OCSP Response	Maximum time to wait for a response from the OCSP responder. Valid range is from 1 second to 10 minutes. Specify a shorter duration to reduce delays in end user access to HTTPS requests in the event that the OCSP responder is unavailable.
Use upstream proxy for OCSP checking	Group Name of the upstream proxies.
Servers exempt from upstream proxy	IP addresses or hostnames of the servers to exempt. May be left blank.

Step 6 **Submit** and **Commit Changes**.

Trusted Root Certificates

The Web Security appliance ships with and maintains a list of trusted root certificates. Web sites with trusted certificates do not require decryption.

You can manage the trusted certificate list, adding certificates to it and functionally removing certificates from it. While the Web Security appliance does not delete certificates from the master list, it allows you to override trust in a certificate, which functionally removes the certificate from the trusted list.

Adding Certificates to the Trusted List

Before you begin

- Verify that the HTTPS Proxy is enabled. See [Enabling the HTTPS Proxy, page 11-3](#)

-
- Step 1** Security Services > HTTPS Proxy.
- Step 2** Click **Manage Trusted Root Certificates**.
- Step 3** Click **Import**.
- Step 4** Click **Browse** and navigate to the certificate file.
- Step 5** **Submit** and **Commit Changes**.

Look for the certificate you uploaded in the **Custom Trusted Root Certificates** list.

Removing Certificates from the Trusted List

-
- Step 1** Select **Security Services > HTTPS Proxy**.
- Step 2** Click **Manage Trusted Root Certificates**.
- Step 3** Select the **Override Trust** checkbox corresponding to the certificate you wish to remove from the list.
- Step 4** **Submit** and **Commit Changes**.
-

Routing HTTPS Traffic

The ability of AsyncOS to route HTTPS transactions based on information stored in client headers is limited and is different for transparent and explicit HTTPS.

Option	Description
Transparent HTTPS	In the case of transparent HTTPS, AsyncOS does not have access to information in the client headers. Therefore, AsyncOS cannot enforce routing policies that rely on information in client headers.
Explicit HTTPS	In the case of explicit HTTPS, AsyncOS has access to the following information in client headers: <ul style="list-style-type: none"> • URL • Destination port number Therefore, for explicit HTTPS transactions, it is possible to match a routing policy based on URL or port number.

Troubleshooting Decryption/HTTPS/Certificates

- [Accessing HTTPS Sites Using Routing Policies with URL Category Criteria, page A-5](#)
- [HTTPS with IP-based Surrogates and Transparent Requests, page A-5](#)
- [Bypassing Decryption for Particular Websites, page A-5](#)
- [Alert: Problem with Security Certificate, page A-6](#)



Scan Outbound Traffic for Existing Infections

- [Overview of Scanning Outbound Traffic, page 12-1](#)
- [Understanding Upload Requests, page 12-2](#)
- [Creating Outbound Malware Scanning Policies, page 12-3](#)
- [Controlling Upload Requests, page 12-4](#)
- [Logging, page 12-6](#)

Overview of Scanning Outbound Traffic

To prevent malicious data from leaving the network, the Web Security appliance provides the Outbound Malware Scanning feature. Using policy groups, you can define which uploads are scanned for malware, which anti-malware scanning engines to use for scanning, and which malware types to block.

The Cisco IronPort Dynamic Vectoring and Streaming (DVS) engine scans transaction requests as they leave the network. By working with the Cisco IronPort DVS engine, the Web Security appliance enables you to prevent users from unintentionally uploading malicious data.

You can perform the following tasks:

Task	Link to Task
Create policies to block malware	Creating Outbound Malware Scanning Policies, page 12-4
Assign upload requests to outbound malware policy groups	Controlling Upload Requests, page 12-6

User Experience with Blocked Requests

When the Cisco IronPort DVS engine blocks an upload request, the Web Proxy sends a block page to the end user. However, not all websites display the block page to the end user. Some Web 2.0 websites display dynamic content using javascript instead of a static webpage and are not likely to display the block page. Users are still properly blocked from uploading malicious data, but they may not always be informed of this by the website.

Understanding Upload Requests

Outbound Malware Scanning Policies define whether or not the Web Proxy blocks HTTP requests and decrypted HTTPS connections for transactions that upload data to a server (upload requests). An upload request is an HTTP or decrypted HTTPS request that has content in the request body.

When the Web Proxy receives an upload request, it compares the request to the Outbound Malware Scanning policy groups to determine which policy group to apply. After it assigns the request to a policy group, it compares the request to the policy group's configured control settings to determine whether to block the request or monitor the request. When an Outbound Malware Scanning Policy determines to monitor a request, it is evaluated against the Access Policies, and the final action the Web Proxy takes on the request is determined by the applicable Access Policy.


Note

Upload requests that try to upload files with a size of zero (0) bytes are not evaluated against Outbound Malware Scanning Policies.

Criteria for Group Membership

Each client request is assigned to an Identity and is then evaluated against the other policy types to determine to which policy group it belongs for each type. The Web Proxy applies the configured policy control settings to a client request based on the client request's policy group membership.

The Web Proxy follows a specific process for matching the group membership criteria. It considers the following factors for group membership:

Criteria	Description
Identity	Each client request either matches an Identity, fails authentication and is granted guest access, or fails authentication and is terminated
Authorized users	If the assigned Identity requires authentication, the user must be in the list of authorized users in the Outbound Malware Scanning Policy group to match the policy group. The list of authorized users can be any of the specified groups or users or can be guest users if the Identity allows guest access
Advanced options	You can configure several advanced options for Outbound Malware Scanning Policy group membership. Some options, such as proxy port and URL category, can also be defined within the Identity. When an advanced option is configured in the Identity, it is not configurable in the Outbound Malware Scanning Policy group level

Matching Client Requests to Outbound Malware Scanning Policy Groups

The Web Proxy compares the upload request status to the membership criteria of the first policy group. If they match, the Web Proxy applies the policy settings of that policy group.

If they do not match, the Web Proxy compares the upload request to the next policy group. It continues this process until it matches the upload request to a user defined policy group. If it does not match a user defined policy group, it matches the global policy group. When the Web Proxy matches the upload request to a policy group or the global policy group, it applies the policy settings of that policy group.

Creating Outbound Malware Scanning Policies

You can create Outbound Malware Scanning Policy groups based on combinations of several criteria, such as one or more Identities or the URL category of the destination site. You must define at least one criterion for policy group membership. When you define multiple criteria, the upload request must meet all criteria to match the policy group. However, the upload request needs to match only one of the configured Identities.

Step 1 Choose **Web Security Manager > Outbound Malware Scanning**.

Step 2 Click **Add Policy**.

Step 3 Enter a name and an optional description for the policy group.



Note Each policy group name must be unique and only contain alphanumeric characters or the space character.

Step 4 In the Insert Above Policy field, select where in the policies table to place the policy group.

When configuring multiple policy groups, you must specify a logical order for each group.

Step 5 In the **Identities and Users** section, select one or more Identity groups to apply to this policy group.

Step 6 (Optional) Expand the Advanced section to define additional membership requirements.

Step 7 To define policy group membership by any of the advanced options, click the link for the advanced option and configure the option on the page that appears.

Advanced Option	Description
Protocols	<p>Choose whether or not to define policy group membership by the protocol used in the client request. Select the protocols to include.</p> <p>“All others” means any protocol not listed above this option.</p> <p>Note When the HTTPS Proxy is enabled, only Decryption Policies apply to HTTPS transactions. You cannot define policy membership by the HTTPS protocol for Access, Routing, Outbound Malware Scanning, Data Security, or External DLP Policies.</p>
Proxy Ports	<p>Choose whether or not to define policy group membership by the proxy port used to access the Web Proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas.</p> <p>For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port.</p> <p>If you define policy group membership by the proxy port when client requests are transparently redirected to the appliance, some requests might be denied.</p> <p>Note If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</p>

Advanced Option	Description
Subnets	<p>Choose whether or not to define policy group membership by subnet or other addresses.</p> <p>You can select to use the addresses that may be defined with the associated Identity, or you can enter specific addresses here.</p> <p>Note If the Identity associated with this policy group defines its membership by addresses, then in this policy group you must enter addresses that are a subset of the addresses defined in the Identity. Adding addresses in the policy group further narrows down the list of transactions that match this policy group.</p>
URL Categories	<p>Choose whether or not to define policy group membership by URL categories. Select the user defined or predefined URL categories.</p> <p>Note If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</p>
User Agents	<p>Choose whether or not to define policy group membership by the user agent used in the client request. You can select some commonly defined browsers, or define your own using regular expressions. Choose whether this policy group should apply to the selected user agents or to any user agent that is not in the list of selected user agents.</p> <p>Note If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</p>
User Location	<p>Choose whether or not to define policy group membership by user location, either remote or local.</p>

Step 8 Submit your changes.

Step 9 Configure Outbound Malware Scanning Policy group control settings to define how the Web Proxy handles transactions.

The new Outbound Malware Scanning Policy group automatically inherits global policy group settings until you configure options for each control setting.

Step 10 **Submit and Commit Changes.**

Controlling Upload Requests

Each upload request is assigned to an Outbound Malware Scanning Policy group and inherits the control settings of that policy group. After the Web Proxy receives the upload request headers, it has the information necessary to decide if it should scan the request body. The DVS engine scans the request and returns a verdict to the Web Proxy. The block page appears to the end user, if applicable.

Step 1 Choose **Web Security Manager > Outbound Malware Scanning**.

Step 2 In the Destinations column, click the link for the policy group you want to configure.

- Step 3** In the **Edit Destination Settings** section, select “Define Destinations Scanning Custom Settings” from the drop-down menu.
- Step 4** In the **Destinations to Scan** section, select one of the following:

Option	Description
Do not scan any uploads	The DVS engine scans no upload requests. All upload requests are evaluated against the Access Policies
Scan all uploads	The DVS engine scans all upload requests. The upload request is blocked or evaluated against the Access Policies, depending on the DVS engine scanning verdict
Scan uploads to specified custom URL categories	The DVS engine scans upload requests that belong in specific custom URL categories. The upload request is blocked or evaluated against the Access Policies, depending on the DVS engine scanning verdict. Click Edit custom categories list to select the URL categories to scan

- Step 5** Submit your changes.
- Step 6** In the Anti-Malware Filtering column, click the link for the policy group.
- Step 7** In the Anti-Malware Settings section, select “Define Anti-Malware Custom Settings”.
- Step 8** In the Cisco IronPort DVS Anti-Malware Settings section, select which anti-malware scanning engines to enable for this policy group.
- Step 9** In the Malware Categories section, select whether to monitor or block the various malware categories. The categories listed in this section depend on which scanning engines you enable.



Note URL transactions are categorized as unscannable when the configured maximum time setting is reached or when the system experiences a transient error condition. For example, transactions might be categorized as unscannable during scanning engine updates or AsyncOS upgrades. The malware scanning verdicts SV_TIMEOUT and SV_ERROR are considered unscannable transactions.

- Step 10** **Submit and Commit Changes.**

Logging

The access logs indicate whether or not the DVS engine scanned an upload request for malware. The scanning verdict information section of each access log entry includes values for the DVS engine activity for scanned uploads. You can also add one of the fields to the W3C or access logs to more easily find this DVS engine activity:

Table 12-1 Log Fields in W3C Logs and Format Specifiers in Access Logs

W3C Log Field	Format Specifier in Access Logs
x-req-dvs-scanverdict	%X2
x-req-dvs-threat-name	%X4
x-req-dvs-verdictname	%X3

When the DVS engine marks an upload request as being malware and it is configured to block malware uploads, the ACL decision tag in the access logs is BLOCK_AMW_REQ.

However, when the DVS engine marks an upload request as being malware and it is configured to *monitor* malware uploads, the ACL decision tag in the access logs is actually determined by the Access Policy applied to the transaction.

To determine whether or not the DVS engine scanned an upload request for malware, view the results of the DVS engine activity in the scanning verdict information section of each access log entry.



Configuring Security Services

- [Overview of Configuring Security Services, page 13-1](#)
- [Overview of Web Reputation Filters, page 13-2](#)
- [Overview of Anti-Malware Scanning, page 13-4](#)
- [Understanding Adaptive Scanning, page 13-7](#)
- [Enabling Web Reputation and Anti-Malware Anti-Malware and Reputation Filters, page 13-8](#)
- [Configuring Web Reputation and Anti-Malware Anti-Malware and Reputation in Policies, page 13-10](#)
- [Maintaining the Database Tables, page 13-15](#)
- [Logging, page 13-15](#)
- [Caching, page 13-16](#)
- [Malware Category Descriptions, page 13-17](#)

Overview of Configuring Security Services

The Web Security appliance uses security components to protect end users from a range of malware threats. You can configure anti-malware and web reputation settings for each policy group. When you configure Access Policies, you can also have AsyncOS for Web choose a combination of anti-malware scanning and web reputation scoring to use when determining what content to block.

To protect end users from malware, you enable these features on the appliance, and then configure anti-malware and web reputation settings per policy.

Option	Description	Link
Anti-malware scanning	Works with multiple anti-malware scanning engines integrated on the appliance to block malware threats	Overview of Anti-Malware Scanning, page 13-4

Option	Description	Link
Web Reputation Filters	Analyzes web server behavior and determines whether the URL contains URL-based malware	Overview of Web Reputation Filters, page 13-2
Advanced Malware Protection	Protects from threats in downloaded files by evaluating file reputation and by analyzing file characteristics.	Overview of File Reputation Filtering and File Analysis, page 16-2

Related Topics

- [Enabling Web Reputation and Anti-Malware Anti-Malware and Reputation Filters, page 13-8](#)
- [Related Topics, page 13-10](#)
- [Understanding Adaptive Scanning, page 13-7](#)

Overview of Web Reputation Filters

Web Reputation Filters assigns a web-based reputation score (WBRs) to a URL to determine the likelihood that it contains URL-based malware. The Web Security appliance uses web reputation scores to identify and stop malware attacks before they occur. You can use Web Reputation Filters with Access, Decryption, and Cisco IronPort Data Security Policies.

Web Reputation Scores

Web Reputation Filters use data to assess the reliability of Internet domains and score the reputation of URLs. The web reputation calculation associates a URL with network parameters to determine the probability that malware exists. The aggregate probability that malware exists is then mapped to a Web Reputation Score between -10 and +10, with +10 being the least likely to contain malware.

Example parameters include the following:

- URL categorization data
- Presence of downloadable code
- Presence of long, obfuscated End-User License Agreements (EULAs)
- Global volume and changes in volume
- Network owner information
- History of a URL
- Age of a URL
- Presence on any block lists
- Presence on any allow lists
- URL typos of popular domains
- Domain registrar information

- IP address information

**Note**

Cisco does not collect identifiable information such as user names, passwords, or client IP addresses.

Understanding How Web Reputation Filtering Works

Web Reputation Scores are associated with an action to take on a URL request. You can configure each policy group to correlate an action to a particular Web Reputation Score. The available actions depend on the policy group type that is assigned to the URL request:

Policy Type	Action
Access Policies	You can choose to block, scan, or allow
Decryption Policies	You can choose to drop, decrypt, or pass through
Cisco IronPort Data Security Policies	You can choose to block or monitor

Web Reputation in Access Policies

When you configure web reputation settings in Access Policies, you can choose to configure the settings manually, or let AsyncOS for Web choose the best options using Adaptive Scanning. When Adaptive Scanning is enabled, you can enable or disable web reputation filtering in each Access Policy, but you cannot edit the Web Reputation Scores.

Score	Action	Description	Example
-10 to -6.0	Block	Bad site. The request is blocked, and no further malware scanning occurs.	<ul style="list-style-type: none"> • URL downloads information without user permission. • Sudden spike in URL volume. • URL is a typo of a popular domain.
-5.9 to 5.9	Scan	Undetermined site. Request is passed to the DVS engine for further malware scanning. The DVS engine scans the request and server response content.	<ul style="list-style-type: none"> • Recently created URL that has a dynamic IP address and contains downloadable content. • Network owner IP address that has a positive Web Reputation Score.
6.0 to 10.0	Allow	Good site. Request is allowed. No malware scanning required.	<ul style="list-style-type: none"> • URL contains no downloadable content. • Reputable, high-volume domain with long history. • Domain present on several allow lists. • No links to URLs with poor reputations.

By default, URLs in an HTTP request that are assigned a Web Reputation Score of +7 are allowed and require no further scanning. However, a weaker score for an HTTP request, such as +3, is automatically forwarded to the Cisco IronPort DVS engine where it is scanned for malware. Any URL in an HTTP request that has a poor reputation is blocked.

Related Topics

- [Understanding Adaptive Scanning, page 13-7](#)

Web Reputation in Decryption Policies

Score	Action	Description
-10 to -9.0	Drop	Bad site. The request is dropped with no notice sent to the end user. Use this setting with caution.
-8.9 to 5.9	Decrypt	Undetermined site. Request is allowed, but the connection is decrypted and Access Policies are applied to the decrypted traffic.
6.0 to 10.0	Pass through	Good site. Request is passed through with no inspection or decryption.

Web Reputation in Cisco IronPort Data Security Policies

Score	Action	Description
-10 to -6.0	Block	Bad site. The transaction is blocked, and no further scanning occurs.
-5.9 to 0.0	Monitor	The transaction will not be blocked based on Web Reputation, and will proceed to content checks (file type and size). Note Sites with no score are monitored.

Overview of Anti-Malware Scanning

The Web Security appliance anti-malware feature uses the Cisco IronPort DVS™ engine in combination with anti-malware scanning engines to stop web-based malware threats. The DVS engine works with the Webroot™, McAfee, and Sophos anti-malware scanning engines.

The scanning engines inspect transactions to determine a malware scanning verdict to pass to the DVS engine. The DVS engine determines whether to monitor or block the request based on the malware scanning verdicts. To use the anti-malware component of the appliance, you must enable anti-malware scanning and configure global settings, and then apply specific settings to different policies.

Related Topics

- [Enabling Web Reputation and Anti-Malware Anti-Malware and Reputation Filters, page 13-8](#)
- [Related Topics, page 13-10](#)

Understanding How the DVS Engine Works

The DVS engine performs anti-malware scanning on URL transactions that are forwarded from the Web Reputation Filters. Web Reputation Filters calculate the probability that a particular URL contains malware, and assign a URL score that is associated with an action to block, scan, or allow the transaction.

When the assigned web reputation score indicates to scan the transaction, the DVS engine receives the URL request and server response content. The DVS engine, in combination with the Webroot and/or Sophos or McAfee scanning engines, returns a malware scanning verdict. The DVS engine uses information from the malware scanning verdicts and Access Policy settings to determine whether to block or deliver the content to the client.

Working with Multiple Malware Verdicts

The DVS engine might determine multiple malware verdicts for a single URL. Multiple verdicts can come from one or both enabled scanning engines:

- **Different verdicts from different scanning engines.** When you enable both Webroot and either Sophos or McAfee, each scanning engine might return different malware verdicts for the same object. When a URL causes multiple verdicts from both enabled scanning engines, the appliance performs the most restrictive action. For example, if one scanning engine returns a block verdict and the other a monitor verdict, the DVS engine always blocks the request.
- **Different verdicts from the same scanning engine.** A scanning engine might return multiple verdicts for a single object when the object contains multiple infections. When a URL causes multiple verdicts from the same scanning engine, the appliance takes action according to the verdict with the highest priority. The following text lists the possible malware scanning verdicts from the highest to the lowest priority.
 - Virus
 - Trojan Downloader
 - Trojan Horse
 - Trojan Phisher
 - Hijacker
 - System monitor
 - Commercial System Monitor
 - Dialer
 - Worm
 - Browser Helper Object
 - Phishing URL
 - Adware
 - Encrypted file
 - Unscannable
 - Other Malware

Webroot Scanning

The Webroot scanning engine inspects objects to determine the malware scanning verdict to send to the DVS engine. The Webroot scanning engine inspects the following objects:

- **URL request.** Webroot evaluates a URL request to determine if the URL is a malware suspect. If Webroot suspects the response from this URL might contain malware, the appliance monitors or blocks the request, depending on how the appliance is configured. If Webroot evaluation clears the request, the appliance retrieves the URL and scans the server response.
- **Server response.** When the appliance retrieves a URL, Webroot scans the server response content and compares it to the Webroot signature database.

McAfee Scanning

The McAfee scanning engine inspects objects downloaded from a web server in HTTP responses. After inspecting the object, it passes a malware scanning verdict to the DVS engine so the DVS engine can determine whether to monitor or block the request.

The McAfee scanning engine uses the following methods to determine the malware scanning verdict:

- Matching virus signature patterns
- Heuristic analysis

Matching Virus Signature Patterns

McAfee uses virus definitions in its database with the scanning engine to detect particular viruses, types of viruses, or other potentially unwanted software. It searches for virus signatures in files. When you enable McAfee, the McAfee scanning engine uses this method to scan server response content.

Heuristic Analysis

Heuristic analysis is a technique that uses general rules, rather than specific rules, to detect new viruses and malware. When the McAfee scanning engine uses heuristic analysis, it looks at the code of an object, applies generic rules, and determines how likely the object is to be virus-like.

Using heuristic analysis increases the possibility of reporting false positives (clean content designated as a virus) and might impact appliance performance. When you enable McAfee, you can choose whether or not to also enable heuristic analysis when scanning objects.

McAfee Categories

McAfee Verdict	Malware Scanning Verdict Category
Known Virus	Virus
Trojan	Trojan Horse
Joke File	Adware
Test File	Virus
Wannabe	Virus
Killed	Virus
Commercial Application	Commercial System Monitor
Potentially Unwanted Object	Adware
Potentially Unwanted Software Package	Adware
Encrypted File	Encrypted File

Sophos Scanning

The Sophos scanning engine inspects objects downloaded from a web server in HTTP responses. After inspecting the object, it passes a malware scanning verdict to the DVS engine so the DVS engine can determine whether to monitor or block the request. You might want to enable the Sophos scanning engine instead of the McAfee scanning engine if McAfee anti-malware software is installed.

Understanding Adaptive Scanning

Adaptive Scanning decides which anti-malware scanning engine (including Advanced Malware Protection scanning for downloaded files) will process the web request. Adaptive Scanning applies the ‘Outbreak Heuristics’ anti-malware category to transactions it identifies as malware prior to running any scanning engines. You can choose whether or not to block these transactions when you configure anti-malware settings on the appliance.

Adaptive Scanning and Access Policies

When Adaptive Scanning is enabled, some anti-malware and reputation settings that you can configure in Access Policies are slightly different:

- You can enable or disable web reputation filtering in each Access Policy, but you cannot edit the Web Reputation Scores.
- You can enable anti-malware scanning in each Access Policy, but you cannot choose which anti-malware scanning engine to enable. Adaptive Scanning chooses the most appropriate engine for each web request.



Note

If Adaptive Scanning is not enabled and an Access Policy has particular web reputation and anti-malware settings configured, and then Adaptive Scanning is enabled, any existing web reputation and anti-malware settings are overridden.

Per-policy Advanced Malware Protection settings are the same whether or not Adaptive Scanning is enabled.

Enabling Anti-Malware and Reputation Filters

Before You Begin

- Check the Web Reputation Filters, DVS engine, and the Webroot, McAfee, and Sophos scanning engines are enabled. By default these should be enabled during system setup.

Step 1 Choose **Security Services > Anti-Malware and Reputation**.

Step 2 Click **Edit Global Settings**.

Step 3 Configure settings as necessary.

Setting	Description
Web Reputation Filtering	Choose whether or not to enable Web Reputation Filtering.
Adaptive Scanning	Choose whether or not to enable Adaptive Scanning. You can only enable Adaptive Scanning when Web Reputation Filtering is enabled.
File Reputation Filtering and File Analysis	See Enabling File Reputation and Analysis Services, page 16-8 .
DVS Engine Object Scanning Limits	Specify a maximum request/response size. The Maximum Object Size value you specify applies to the entire size of requests and responses that might be scanned by security components on the Web Security appliance, such as the Cisco IronPort Data Security Filters or the Webroot scanning engine. When an upload or download size exceeds this size, the security component may abort the scan in progress and may not provide a scanning verdict to the Web Proxy.
Sophos	Choose whether or not to enable the Sophos scanning engine.

Setting	Description
McAfee	<p>Choose whether or not to enable the McAfee scanning engine.</p> <p>When you enable the McAfee scanning engine, you can choose whether or not to enable heuristic scanning.</p> <p>Note Heuristic analysis increases security protection, but can result in false positives and decreased performance.</p>
Webroot	<p>Choose whether or not to enable the Webroot scanning engine.</p> <p>When you enable the Webroot scanning engine, you can configure the Threat Risk Threshold (TRT). The TRT assigns a numerical value to the probability that malware exists.</p> <p>Proprietary algorithms evaluate the result of a URL matching sequence and assign a Threat Risk Rating (TRR). This value is associated with the threat risk threshold setting. If the TRR value is greater than or equal to the TRT, the URL is considered malware and is passed on for further processing.</p> <p>Note Setting the Threat Risk Threshold to a value lower than 90 dramatically increases the rate of URL blocking and denies legitimate requests. Cisco strongly recommends maintaining the TRT default value of 90. The minimum value for a TRT setting is 51.</p>

Step 4 Submit and Commit Changes.

Related Topics

- [Understanding Adaptive Scanning, page 13-7](#)
- [McAfee Scanning, page 13-6](#)

Configuring Anti-Malware and Reputation in Policies

When Anti-Malware and Reputation Filters are enabled on the appliance, you can configure different settings in policy groups. You can enable monitoring or blocking for malware categories based on malware scanning verdicts.

You can configure anti-malware settings in the following policy groups:

Policy Type	Link to Task
Access Policies	Web Reputation and Anti-Malware Anti-Malware and Reputation Settings in Access Policies, page 13-11
Outbound Malware Scanning Policies	Controlling Upload Requests Using Outbound Malware Scanning Policies

You can configure web reputation settings in the following policy groups:

Policy Type	Link to Task
Access Policies	Web Reputation and Anti-Malware Anti-Malware and Reputation Settings in Access Policies, page 13-11
Decryption Policies	Configuring Web Reputation Filter Settings for Decryption Policy Groups, page 13-14
Cisco Data Security Policies	Configuring Web Reputation Filter Settings for Decryption Policy Groups, page 13-14

You can configure Advanced Malware Protection settings only in Access Policies. See [Enabling File Reputation and Analysis Services Per Access Policy, page 16-9](#).

Anti-Malware and Reputation Settings in Access Policies

When Adaptive Scanning is enabled, the web reputation and anti-malware settings you can configure for Access Policies are slightly different than when Adaptive Scanning is turned off.



Note

If your deployment includes a Security Management appliance, and you are configuring this feature in a Configuration Master, options on this page depend on whether Adaptive Security is enabled for the relevant configuration master. Check the setting on the Security Management appliance, on the **Web > Utilities > Security Services Display** page.

Related Topics

- [Understanding Adaptive Scanning, page 13-7](#)

Configuring Anti-Malware and Reputation Settings with Adaptive Scanning Enabled

- Step 1** Choose **Web Security Manager > Access Policies**.
- Step 2** Click the **Anti-Malware and Reputation** link for the Access Policy you want to configure.
- Step 3** Under the **Web Reputation and Anti-Malware Settings** section, choose **Define Web Reputation and Anti-Malware Custom Settings**.
This allows you to configure web reputation and anti-malware settings for this Access Policy that differ from the global policy.
- Step 4** In the **Web Reputation Settings** section, choose whether or not to enable Web Reputation Filtering. Adaptive Scanning chooses the most appropriate web reputation score thresholds for each web request.
- Step 5** Configure the settings in the **Advanced Malware Protection Settings** section.
- Step 6** Scroll down to the Cisco DVS Anti-Malware Settings section.

Step 7 Configure the anti-malware settings for the policy as necessary.

Setting	Description
Enable Suspect User Agent Scanning	Choose whether or not to scan traffic based on the user agent field specified in the HTTP request header. When you select this checkbox, you can choose to monitor or block suspect user agents in the Additional Scanning section at the bottom of the page.
Enable Anti-Malware Scanning	Choose whether or not to use the DVS engine to scan traffic for malware. Adaptive Scanning chooses the most appropriate engine for each web request.
Malware Categories	Choose whether to monitor or block the various malware categories based on a malware scanning verdict.
Other Categories	Choose whether to monitor or block the types of objects and responses listed in this section. Note The category Outbreak Heuristics applies to transactions which are identified as malware by Adaptive Scanning prior to running any scanning engines. Note URL transactions are categorized as unscannable when the configured maximum time setting is reached or when the system experiences a transient error condition. For example, transactions might be categorized as unscannable during scanning engine updates or AsyncOS upgrades. The malware scanning verdicts SV_TIMEOUT and SV_ERROR, are considered unscannable transactions.

Step 8 **Submit and Commit Changes.**

Related Topics

- [Malware Category Descriptions, page 13-17](#)

Configuring Anti-Malware and Reputation Settings with Adaptive Scanning Disabled

Step 1 Choose **Web Security Manager > Access Policies**.

Step 2 Click the **Anti-Malware and Reputation** link for the Access Policy you want to configure.

Step 3 Under the **Web Reputation and Anti-Malware Settings** section, choose **Define Web Reputation and Anti-Malware Custom Settings**.

This allows you to configure web reputation and anti-malware settings for this Access Policy that differ from the global policy.

Step 4 Configure the settings in the Web Reputation Settings section.

Step 5 Configure the settings in the **Advanced Malware Protection Settings** section.

Step 6 Scroll down to the Cisco DVS Anti-Malware Settings section.

Step 7 Configure the anti-malware settings for the policy as necessary.

**Note**

When you enable Webroot, Sophos or McAfee scanning, you can choose to monitor or block some additional categories in the Malware categories on this page

Setting	Description
Enable Suspect User Agent Scanning	Choose whether or not to enable the appliance to scan traffic based on the user agent field specified in the HTTP request header. When you select this checkbox, you can choose to monitor or block suspect user agents in the Additional Scanning section at the bottom of the page.
Enable Webroot	Choose whether or not to enable the appliance to use the Webroot scanning engine when scanning traffic.
Enable Sophos or McAfee	Choose whether or not to enable the appliance to use either the Sophos or McAfee scanning engine when scanning traffic.
Malware Categories	Choose whether to monitor or block the various malware categories based on a malware scanning verdict. The categories listed in this section depend on which scanning engines you enable above.
Other Categories	Choose whether to monitor or block the types of objects and responses listed in this section. Note URL transactions are categorized as unscannable when the configured maximum time setting is reached or when the system experiences a transient error condition. For example, transactions might be categorized as unscannable during scanning engine updates or AsyncOS upgrades. The malware scanning verdicts SV_TIMEOUT and SV_ERROR, are considered unscannable transactions.

Step 8 Submit and Commit Changes.**Related Topics**

- [Configuring Web Reputation Score Thresholds for Access Policies, page 13-14](#)
- [Malware Category Descriptions, page 13-17](#)

Configuring Web Reputation Scores

When you install and set up the Web Security appliance, it has default settings for Web Reputation Scores. However, you can modify threshold settings for web reputation scoring to fit your organization's needs. You configure the web reputation filter settings for each policy group.

Configuring Web Reputation Score Thresholds for Access Policies

- Step 1** Choose **Web Security Manager > Access Policies**.
- Step 2** Click the link under the Anti-Malware and Reputation column for the Access Policy group you want to edit.

- Step 3** Under the Web Reputation and Anti-Malware Settings section, choose **Define Web Reputation and Anti-Malware Custom Settings**.
- This allows you to configure web reputation and anti-malware settings for this Access Policy that differ from the global policy.
- Step 4** Verify the Enable Web Reputation Filtering field is enabled.
- Step 5** Move the markers to change the range for URL block, scan, and allow actions.
- Step 6** **Submit and Commit Changes**.



Note You can edit the web reputation score thresholds in Access Policies when Adaptive Scanning is disabled

Configuring Web Reputation Filter Settings for Decryption Policy Groups

- Step 1** Choose **Web Security Manager > Decryption Policies**.
- Step 2** Click the link under the Web Reputation column for the Decryption Policy group you want to edit.
- Step 3** Under the Web Reputation Settings section, choose **Define Web Reputation Custom Settings**. This allows you to override the web reputation settings from the Global Policy Group.
- Step 4** Verify the Enable Web Reputation Filtering field is checked.
- Step 5** Move the markers to change the range for URL drop, decrypt, and pass through actions.
- Step 6** In the **Sites with No Score** field, choose the action to take on request for sites that have no assigned Web Reputation Score.
- Step 7** **Submit and Commit Changes**.

Configuring Web Reputation Filter Settings for Data Security Policy Groups

- Step 1** Choose **Web Security Manager > Cisco IronPort Data Security**.
- Step 2** Click the link under the Web Reputation column for the Data Security Policy group you want to edit.
- Step 3** Under the Web Reputation Settings section, choose **Define Web Reputation Custom Settings**.
This allows you to override the web reputation settings from the Global Policy Group.
- Step 4** Move the marker to change the range for URL block and monitor actions.
- Step 5** **Submit and Commit Changes**.



Note Only negative and zero values can be configured for web reputation threshold settings for Cisco IronPort Data Security Policies. By definition, all positive scores are monitored

Maintaining the Database Tables

The web reputation, Webroot, Sophos, and McAfee databases periodically receive updates from the Cisco IronPort update server (<https://update-manifests.ironport.com>). Server updates are automated and the update interval is set by the server.

The Web Reputation Database

The Web Security appliance maintains a filtering database that contains statistics and information about how different types of requests are handled. The appliance can also be configured to send web reputation statistics to a Cisco SensorBase Network server. SensorBase server information is leveraged with data feeds from the SensorBase Network and the information is used to produce a Web Reputation Score.

Logging

The access log file records the information returned by the Web Reputation Filters and the DVS engine for each transaction. The scanning verdict information section in the access logs includes many fields to help understand the cause for the action applied to a transaction. For example, some fields display the web reputation score or the malware scanning verdict Sophos passed to the DVS engine.

Logging Adaptive Scanning

Custom Field in Access Logs	Custom Field in W3C Logs	Description
%X6	x-as-malware-threat-name	The anti-malware name returned by Adaptive Scanning. If the transaction is not blocked, this field returns a hyphen ("-"). This variable is included in the scanning verdict information (in the angled brackets at the end of each access log entry).

Transactions blocked and monitored by the adaptive scanning engine use the ACL decision tags:

- BLOCK_AMW_RESP
- MONITOR_AMW_RESP

Caching

The following guidelines explain how AsyncOS uses the cache while scanning for malware:

- AsyncOS only caches objects if the entire object downloads. If malware is blocked during scanning, the whole object is not downloaded and therefore is not cached.
- AsyncOS scans content whether it is retrieved from the server or from the web cache.
- The length of time that content is cached varies with many factors - there is no default.
- AsyncOS rescans content when signatures are updated.

Malware Category Descriptions

Malware Type	Description
Adware	Adware encompasses all software executables and plug-ins that direct users towards products for sale. These programs may also change security settings making it impossible for users to make changes to their system settings.
Browser Helper Object	A browser helper object is a browser plug-in that may perform a variety of functions related to serving advertisements or hijacking user settings.
Commercial System Monitor	A commercial system monitor is a piece of software with system monitor characteristics that can be obtained with a legitimate license through legal means.
Dialer	A dialer is a program that utilizes your modem or another type of Internet access to connect you to a phone line or a site that causes you to accrue long distance charges to which you did not provide your full consent.
Generic Spyware	Spyware is a type of malware installed on computers that collects small pieces of information about users without their knowledge.
Hijacker	A hijacker modifies system settings or any unwanted changes to a user's system that may direct them to a website or run a program without a users consent.
Known Malicious and High-Risk Files	These are files that were identified as threats by the Advanced Malware Protection file reputation service.
Other Malware	This category is used to catch all other malware and suspicious behavior that does not exactly fit in one of the other defined categories.
Phishing URL	A phishing URL is displayed in the browser address bar. In some cases, it involves the use of domain names and resembles those of legitimate domains.
PUA	Potentially Unwanted Application. A PUA is an application that is not malicious, but may be considered to be undesirable.
System Monitor	A system monitor encompasses any software that performs one of the following: <ul style="list-style-type: none"> • Overtly or covertly records system processes and/or user action. • Makes those records available for retrieval and review at a later time.
Trojan Downloader	A trojan downloader is a Trojan that, after installation, contacts a remote host/site and installs packages or affiliates from the remote host.
Trojan Horse	A trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves.
Trojan Phisher	A trojan phisher may sit on an infected computer waiting for a specific web page to be visited or may scan the infected machine looking for user names and passwords.
Virus	A virus is a program or piece of code that is loaded onto your computer without your knowledge.
Worm	A worm is program or algorithm that replicates itself over a computer network and performs malicious actions.



File Reputation Filtering and File Analysis

- [Overview of File Reputation Filtering and File Analysis, page 16-2](#)
- [Configuring File Reputation and Analysis Features, page 16-6](#)
- [File Reputation and File Analysis Reporting and Tracking, page 16-13](#)
- [Taking Action When File Threat Verdicts Change, page 16-18](#)
- [Troubleshooting File Reputation and Analysis, page 16-18](#)

Overview of File Reputation Filtering and File Analysis

Advanced Malware Protection uses cloud-based services to protect against zero-day and targeted file-based threats by:

- Obtaining each file's reputation.
- Analyzing behavior of certain files with unknown reputations.
- Notifying you about files that are determined to be threats after they have entered your network

These features are available only for file downloads. Uploaded files are not evaluated.

File Threat Verdict Updates

Because Advanced Malware Protection is focused on targeted and zero-day threats, threat verdicts can change as new information emerges.

A file may initially be evaluated as unknown or clean, and the user may thus be allowed to access the file. If the threat verdict changes, you will be alerted, and the file and its new verdict appear in the AMP Verdict Updates report. You can investigate the point-of-entry transaction as a starting point to remediating any impacts of the threat.

Verdicts can also change from malicious to clean.

When the appliance processes subsequent instances of the same file, the updated verdict is immediately applied.

Related Topics

- [File Reputation and File Analysis Reporting and Tracking, page 16-13](#)
- [Taking Action When File Threat Verdicts Change, page 16-18](#)

File Processing Overview

First, the web site from which the file is downloaded is evaluated against the Web Based Reputation Service (WBRS).

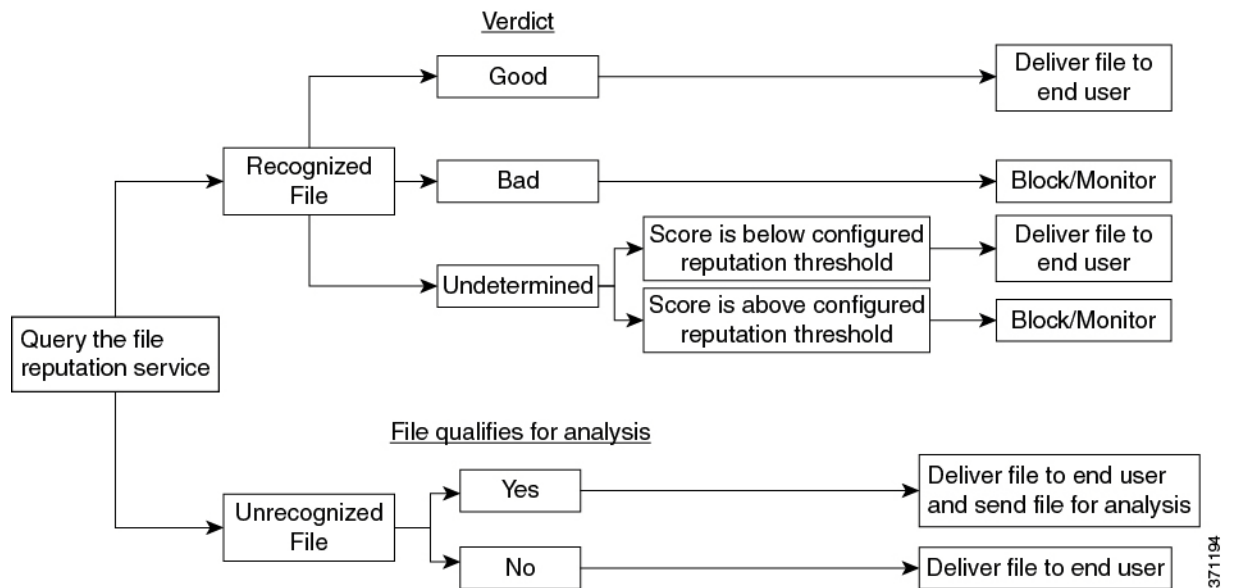
If the web reputation score of the site is in the range configured to “Scan,” the appliance simultaneously scans the transaction for malware and queries the cloud-based service for the reputation of the file. (If the site’s reputation score is in the “Block” range, the transaction is handled accordingly and there is no need to process the file further.) If malware is found during scanning, the transaction is blocked regardless of the reputation of the file.

If Adaptive Scanning is also enabled, file reputation evaluation and file analysis are included in Adaptive Scanning.

Communications between the appliance and the file reputation service are encrypted and protected from tampering.

After a file’s reputation is evaluated:

- If the file is known to the file reputation service and is determined to be clean, the file is released to the end user.
- If the file reputation service returns a verdict of malicious, then the appliance applies the action that you have specified for such files.
- If the file is known to the reputation service but there is insufficient information for a definitive verdict, the reputation service returns a threat score based on characteristics of the file such as threat fingerprint and behavioral analysis. If this score meets or exceeds the configured reputation threshold (you need not change the default), the appliance applies the action that you have configured in the access policy for malicious or high-risk files.
- If the reputation service has no information about the file, and the file does not meet the criteria for analysis, the file is considered clean and the file is released to the end user.
- If the reputation service has no information about the file, and the file meets the criteria for files that can be analyzed (see [Which Files Can Be Evaluated and Analyzed?](#), page 16-5), then the file is considered clean and is sent for analysis.
- If file reputation information is unavailable, for example because the connection with the cloud service timed out, the file is considered clean and is released to the end user.



If the file is sent for analysis:

- Files are sent using SSL/TLS.
- Analysis normally takes minutes, but may take longer.
- Information about every file analyzed is added to the reputation database. File analysis results contribute to the reputation of the file.

For information about verdict updates, see [File Threat Verdict Updates, page 16-2](#).

Related Topics

- [File Reputation and File Analysis Reporting and Tracking, page 16-13](#)

Which Files Can Be Evaluated and Analyzed?

The reputation service evaluates most file types. File type identification is determined by file content and is not dependent on the filename extension.

Some files with unknown reputation can be analyzed for threat characteristics.

Additional criteria apply, including some that are dynamically determined. For current information, see the Release Notes for your AsyncOS version, available from

<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html>

FIPS Compliance

File reputation scanning and file analysis are FIPS compliant.

Configuring File Reputation and Analysis Features

- [Requirements for Communication with File Reputation and Analysis Services, page 16-7](#)
- [Enabling File Reputation and Analysis Services, page 16-8](#)
- [Enabling File Reputation and Analysis Services Per Access Policy, page 16-9](#)
- [Ensuring That You Receive Alerts, page 16-12](#)
- [Configuring Centralized Reporting for Advanced Malware Protection Features, page 16-12](#)

Requirements for Communication with File Reputation and Analysis Services

- All Web Security appliances that use these services must be able to connect to them directly over the internet. An upstream proxy is not supported.
- By default, communication with file reputation and analysis services is routed through the Management port (M1) on the appliance. If your appliance does not route data through the management port, see [Routing Traffic to File Reputation and File Analysis Servers Through a Data Interface, page 16-7](#).
- Communication with cloud services for file reputation and analysis occurs over IPv4.
- The following firewall ports must be open:

Firewall Ports	Description	Protocol	In/Out	Hostname	Appliance Interface
32137	Access to cloud services for obtaining file reputation.	TCP	Out	As configured in Security Services > Anti-Malware and Reputation, Advanced section, Cloud Server Pool parameter.	Management, unless a static route is configured to route this traffic through a data port.
443	Access to cloud services for file analysis.	TCP	Out	As configured in Security Services > Anti-Malware and Reputation, Advanced section.	

Routing Traffic to File Reputation and File Analysis Servers Through a Data Interface

If the appliance is configured to restrict the management port to appliance management services only (on the Network > Interfaces page), configure the appliance to route file reputation and analysis traffic through the data port instead.

Add routes for data traffic on the Network > Routes page. For general requirements and instructions, see [Configuring TCP/IP Traffic Routes, page 3-18](#).

For Connection To	Destination Network	Gateway
The file reputation service	IP addresses of the Cloud Server Pool, as configured in Security Services > Anti-Malware and Reputation, Advanced section.	IP address of the gateway for the data port
The file analysis service	IP address of the File Analysis Server, as configured in Security Services > Anti-Malware and Reputation, Advanced section.	IP address of the gateway for the data port

Related Topics

- [Configuring TCP/IP Traffic Routes, page 3-18](#)

Enabling File Reputation and Analysis Services

Before You Begin

- Separate feature keys are required for the file reputation service and the file analysis service.
- Meet the [Requirements for Communication with File Reputation and Analysis Services, page 16-7](#).

Procedure

-
- Step 1** Select **Security Services > Anti-Malware and Reputation** .
- Step 2** Click **Edit Global Settings**.
- Step 3** In the **Advanced Malware Protection Services** section, select **Enable File Reputation Filtering**.
- Step 4** Accept the license agreement if presented.
- Step 5** In the **Advanced Malware Protection Services** section, select **Enable File Analysis**.



Note Do not change Advanced settings without guidance from Cisco support.

- Step 6** Submit and commit your changes.
-

Enabling File Reputation and Analysis Services Per Access Policy

Procedure

-
- Step 1** Select **Web Security Manager > Access Policies**.
- Step 2** Click the link in the **Anti-Malware and Reputation** column for a policy in the table.
- Step 3** In the **Advanced Malware Protection Settings** section, select **Enable File Reputation Filtering and File Analysis**.

If File Analysis is not enabled globally, only File Reputation Filtering is offered.

- Step 4** Select an action for **Known Malicious and High-Risk Files**: **Monitor** or **Block**.
The default is Monitor.
- Step 5** Submit and commit your changes.
-

Ensuring That You Receive Alerts

Ensure that the appliance is configured to send you alerts related to Advanced Malware Protection.

You will receive alerts when:

Alert Description	Type	Severity
Feature keys expire	(As is standard for all features)	
The file reputation service is unreachable	Anti-Malware	Warning
The file analysis service is unreachable	Anti-Malware	Warning
A file reputation verdict changes	Anti-Malware	Info

Related Topics

- [Multiple Alerts About Failed File Reputation Queries](#), page 16-19
- [File Upload for Analysis Fails Repeatedly](#), page 16-20
- [Taking Action When File Threat Verdicts Change](#), page 16-18

Configuring Centralized Reporting for Advanced Malware Protection Features

If you will centralize reporting on a Security Management appliance, see important configuration requirements in the Advanced Malware Protection sections in the web reporting chapter of the online help or user guide for your management appliance.

File Reputation and File Analysis Reporting and Tracking

- [Identifying Files by SHA-256 Hash](#), page 16-13
- [File Reputation and File Analysis Report Pages](#), page 16-14
- [Viewing File Reputation Filtering Data in Other Reports](#), page 16-15
- [About Web Message Tracking and Advanced Malware Protection Features](#), page 16-16

Identifying Files by SHA-256 Hash

Because filenames can easily be changed, the appliance generates an identifier for each file using a Secure Hash Algorithm (SHA-256). If an appliance processes the same file with different names, all instances are recognized as the same SHA-256. If multiple appliances process the same file, all instances of the file have the same SHA-256 identifier.

In most reports, files are listed by their SHA-256 value (in an abbreviated format). To identify the filenames associated with a malware instance in your organization, select Reporting > Advanced Malware Protection and click an SHA-256 link in the table. The details page shows associated filenames.

File Reputation and File Analysis Report Pages

Report	Description
Advanced Malware Protection	<p>Shows file-based threats that were identified by the file reputation service.</p> <p>To see the users who tried to access each SHA, and the filenames associated with that SHA-256, click a SHA-256 in the table.</p> <p>Clicking the link at the bottom of Malware Threat File Details report page displays all instances of the file in Web Tracking that were encountered within the maximum available time range, regardless of the time range selected for the report.</p> <p>For files with changed verdicts, see the AMP Verdict updates report. Those verdicts are not reflected in the Advanced Malware Protection report.</p>
File Analysis	<p>Displays the time and verdict (or interim verdict) for each file sent for analysis.</p> <p>To view more than 1000 File Analysis results, export the data as a .csv file.</p> <p>Drill down to view detailed analysis results, including the threat characteristics and score for each file.</p> <p>You can also search the cloud service for additional information about an SHA. The link is on the result details page.</p>
AMP Verdict Updates	<p>Lists the files processed by this appliance for which the verdict has changed since the transaction was processed. For information about this situation, see File Threat Verdict Updates, page 16-2.</p> <p>To view more than 1000 verdict updates, export the data as a .csv file.</p> <p>In the case of multiple verdict changes for a single SHA-256, this report shows only the latest verdict, not the verdict history.</p> <p>Clicking an SHA-256 link displays the Malware Threat Files page, which displays data only if the file was initially determined to contain malware.</p> <p>To view all affected transactions for a particular SHA-256 within the maximum available time range (regardless of the time range selected for the report) click the link at the bottom of the Malware Threat Files page.</p>

Viewing File Reputation Filtering Data in Other Reports

Data for file reputation and analysis is available in other reports where relevant. A "Blocked by Advanced Malware Protection" column may be hidden by default in applicable reports. To display additional columns, click the Columns link below the table.

The Report by User Location includes an Advanced Malware Protection tab.

About Web Tracking and Advanced Malware Protection Features

When searching for file threat information in Web Tracking, keep the following points in mind:

- To search for malicious files found by the file reputation service, select **Known Malicious and High-Risk Files** for the **Filter by Malware Category** option in the Malware Threat area in the Advanced section in Web Tracking.
- Web Tracking includes only information about file reputation processing and the original file reputation verdicts returned at the time a transaction was processed. For example, if a file was initially found to be clean, then a verdict update found the file to be malicious, only the clean verdict appears in Tracking results.

"Block - AMP" in search results means the transaction was blocked because of the file's reputation verdict.

In Tracking details, the "AMP Threat Score" is the best-effort score that the cloud reputation service provides when it cannot determine a clear verdict for the file. In this situation, the score is between 1 and 100. (Ignore the AMP Threat Score if an AMP Verdict is returned or if the score is zero.) The appliance compares this score to the threshold score (configured on the Security Services > Anti-Malware and Reputation page) to determine what action to take. By default, files with scores between 60 and 100 are considered malicious. Cisco does not recommend changing the default threshold score. The WBRs score is the reputation of the site from which the file was downloaded; this score is not related to the file reputation.

- Verdict updates are available only in the AMP Verdict Updates report. The original transaction details in Web Tracking are not updated with verdict changes. To see transactions involving a particular file, click a SHA-256 in the verdict updates report.
- Information about File Analysis, including analysis results and whether or not a file was sent for analysis, are available only in the File Analysis report.

Additional information about an analyzed file may be available from the cloud. To view any available File Analysis information for a file, select **Reporting > File Analysis** and enter the SHA-256 to search for the file, or click the SHA-256 link in Web Tracking details. If the File Analysis service has analyzed the file from any source, you can see the details. Results are displayed only for files that have been analyzed.

If the appliance processed a subsequent instance of a file that was sent for analysis, those instances will appear in Web Tracking search results.

Taking Action When File Threat Verdicts Change

Procedure

-
- Step 1** View the AMP Verdict Updates report.

- Step 2** Click the relevant SHA-256 link to view web tracking data for all transactions involving that file that end users were allowed to access.
- Step 3** Using the tracking data, identify the users that may have been compromised, as well as information such as the file names involved in the breach and the web site from which the file was downloaded.
- Step 4** Check the File Analysis report to see if this SHA-256 was sent for analysis, to understand the threat behavior of the file in more detail.
-

Related Topics

- [File Threat Verdict Updates, page 16-2](#)

Troubleshooting File Reputation and Analysis

- [Log Files, page 16-18](#)
- [Multiple Alerts About Failed File Reputation Queries, page 16-19](#)
- [File Upload for Analysis Fails Repeatedly, page 16-20](#)

Log Files

In logs:

- `AMP` and `amp` refer to the file reputation service or engine.
- `Retrospective` refers to verdict updates.
- `VRT` and `sandboxing` refer to the file analysis service.

Advanced Malware Protection information is logged in Access Logs or in AMP Engine Logs. For more information, see the chapter on monitoring system activity through logs.

Multiple Alerts About Failed File Reputation Queries

Problem You receive multiple alerts about failures to query the file reputation service.

Solution

- Ensure that you have met the requirements in [Requirements for Communication with File Reputation and Analysis Services, page 16-7](#).
- Check for network issues that may prevent the appliance from communicating with the cloud services.
- Increase the Query Timeout value:

Select **Security Services > Anti-Malware and Reputation** . The Query Timeout value is in the Advanced settings area of the **Advanced Malware Protection Services** section.

File Upload for Analysis Fails Repeatedly

Problem You receive an alert that uploading files for analysis has failed repeatedly.

Solution

- Ensure that you have met the requirements in [Requirements for Communication with File Reputation and Analysis Services, page 16-7](#).
- Check your network for issues.
- If the problem persists, contact Cisco support.



Managing Access to Web Applications

- [Overview of Managing Access to Web Applications, page 14-1](#)
- [Understanding Application Control Settings, page 14-2](#)
- [Enabling the AVC Engine, page 14-3](#)
- [Controlling Bandwidth, page 14-4](#)
- [Controlling Instant Messaging Traffic, page 14-6](#)
- [Viewing AVC Activity, page 14-7](#)

Overview of Managing Access to Web Applications

The AVC engine allows you to create policies to control application activity on the network without having to fully understand the underlying technology of each application. You can configure application control settings in Access Policy groups. You can block or allow applications by application type or a particular application. You can also apply controls to particular application types.

Using Access Policies you can:

- Control application behaviors
- Control the amount of bandwidth used for particular application types
- Notify end-users when they are blocked
- Assign controls to Instant Messaging, Blogging and Social Media applications

To control applications using the AVC engine, perform the following tasks:

Task	Link to Task
Enable the AVC engine	Enabling the AVC Engine, page 14-3
Setting Controls in an Access Policy Group	Configuring Application Control Settings in an Access Policy Group, page 14-4
Limit bandwidth consumed by some application types to control congestion	Controlling Bandwidth, page 14-4
Allow instant messaging traffic, but disallow file sharing using instant messenger	Controlling Instant Messaging Traffic, page 14-6

Understanding Application Control Settings

Controlling applications involves configuring the following elements:

Option	Description
Application types	A category that contains one or more applications
Applications	Particular applications that belong in an application type
Application behaviors	Particular actions or behaviors that users can do within an application that administrators can control. Not all applications include application behaviors you can configure

The Applications Visibility and Control page offers the following views for configuring applications:

- **Browse view.** You can browse for application types. You can use Browse view to configure applications of a particular type at the same time. When an application type is collapsed in Browse view, the summary for the application type lists the final actions for the applications and does not indicate whether the actions are inherited from the global policy or configured in the current Access Policy.
- **Search view.** You can search for applications. You might want to use Search view when the total list of applications is long and you need to quickly find and configure a particular application.



Note

You can configure most of the same control settings in both views. However, you can only configure the bandwidth control limits for application types in Browse view.

When configuration applications, you can choose the following actions:

Option	Description
Block	This action is a final action. Users are prevented from viewing a webpage and instead an end-user notification page displays
Monitor	This action is an intermediary action. The Web Proxy continues comparing the transaction to the other control settings to determine which final action to apply
Restrict	This action indicates that an application behavior is blocked. For example, when you block file transfers for a particular instant messaging application, the action for that application is Restrict

Related topics

- [Viewing AVC Activity, page 14-7](#)

AVC Engine Updates

AsyncOS periodically queries the update servers for new updates to all security service components, including the AVC engine. AVC engine updates can include support for new application types and applications as well as updated support for existing applications if any application behavior changes. By updating the AVC engine in between AsyncOS versions, the Web Security appliance remains flexible without requiring a server upgrade.

AsyncOS for Web assigns the following default actions for the Global Access Policy:

- New application types default to Monitor.
- New application behaviors, such as block file transfer within a particular application, default to Monitor.
- New applications for an existing application type default to the application type default.

**Note**

You can view the AVC engine scanning activity in the Application Visibility report on the **Reporting > Application Visibility** page.

**Note**

In the Global Access Policy, you can set the default action for each application type. You might want to set the default action for each application type so new applications introduced in an Application Visibility and Control engine update automatically inherit the default action.

User Experience with Blocked Requests

When the AVC engine blocks a transaction, the Web Proxy sends a block page to the end user. However, not all websites display the block page to the end user. Some Web 2.0 websites display dynamic content using javascript instead of a static webpage and are not likely to display the block page. Users are still properly blocked from downloading malicious data, but they may not always be informed of this by the website.

Enabling the AVC Engine

Enable the AVC engine when you enable Cisco Web Usage Controls.

-
- Step 1** Choose **Security Services > Acceptable Use Controls**.
 - Step 2** Click **Edit Global Settings**.
 - Step 3** Verify the Enable Acceptable Use Controls property is enabled.
 - Step 4** In the Acceptable Use Controls Service area, select **Cisco Web Usage Controls**, and then select **Enable Application Visibility and Control**.
 - Step 5** **Submit** and **Commit Changes**.

Configuring Application Control Settings in an Access Policy Group

-
- Step 1** Choose **Web Security Manager > Access Policies**.
 - Step 2** Click the link in the policies table under the Applications column for the policy group you want to edit.
 - Step 3** When configuring the Global Access Policy, define the default action for each application type in the **Default Actions for Application Types** section.
 - Step 4** When configuring a user defined Access Policy, choose **Define Applications Custom Settings** in the **Edit Applications Settings** section.
 - Step 5** In the Application Settings area, choose **Browse view** or **Search view** from the drop down menu.
 - Step 6** Configure the action for each application and application behavior.
 - Step 7** Configure the bandwidth controls for each applicable application.
 - Step 8** **Submit** and **Commit Changes**.
-

Related topics

- [Controlling Bandwidth, page 14-4](#)

Controlling Bandwidth

When both the overall limit and user limit applies to a transaction, the most restrictive option applies. You can define bandwidth limits for particular URL categories by defining an Identity group for a URL category and using it in an Access Policy that restricts the bandwidth.

You can define the following bandwidth limits:

Bandwidth limit	Description	Link to Task
Overall	Define an overall limit for all users on the network for the supported application types. The overall bandwidth limit affects the traffic between the Web Security appliance and web servers. It does not limit traffic served from the web cache.	Configuring Overall Bandwidth Limits, page 14-5
User	Define a limit for particular users on the network per application type. User bandwidth limits traffic from web servers as well as traffic served from the web cache.	Configuring User Bandwidth Limits, page 14-5



Note

Defining bandwidth limits only throttles the data going to users. It does not block data based on reaching a quota. The Web Proxy introduces latency into each application transaction to mimic a slower link to the server.

Configuring Overall Bandwidth Limits

-
- Step 1** Choose **Web Security Manager > Overall Bandwidth Limits**
 - Step 2** Click **Edit Settings**.
 - Step 3** Select the **Limit to** option.
 - Step 4** Enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps).
 - Step 5** **Submit** and **Commit Changes**.
-

Configuring User Bandwidth Limits

You can define user bandwidth limits by configuring bandwidth control settings on the Applications Visibility and Control page of Access Policies. You can define the following types of bandwidth controls for users in Access Policies:

Option	Description	Link to task
Default bandwidth limit for an application type	In the Global Access Policy, you can define the default bandwidth limit for all applications of an application type.	Configuring the Default Bandwidth Limit for an Application Type, page 14-5
Bandwidth limit for an application type	In a user defined Access Policy, you can override the default bandwidth limit for the application type defined in the Global Access Policy.	Overriding the Default Bandwidth Limit for an Application Type, page 14-6
Bandwidth limit for an application	In a user defined or Global Access Policy, you can choose to apply the application type bandwidth limit or no limit (exempt the application type limit).	Configuring Bandwidth Controls for an Application, page 14-6

Configuring the Default Bandwidth Limit for an Application Type

-
- Step 1** Choose **Web Security Manager > Access Policies**.
 - Step 2** Click the link in the policies table under the Applications column for the Global Access Policy.
 - Step 3** In the **Default Actions for Application Types** section, click the link next to “Bandwidth Limit” for the application type you want to edit.
 - Step 4** Select **Set Bandwidth Limit** and enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps).
 - Step 5** Click **Apply**.
 - Step 6** **Submit** and **Commit Changes**.
-

Overriding the Default Bandwidth Limit for an Application Type

You can override the default bandwidth limit defined at the Global Access Policy group in the user defined Access Policies. You can only do this in Browse view.

-
- Step 1** Choose **Web Security Manager > Access Policies**.
 - Step 2** Click the link in the policies table under the Applications column for the user defined policy group you want to edit.
 - Step 3** Choose **Define Applications Custom Settings** in the Edit Applications Settings section.
 - Step 4** Click the link next to “Bandwidth Limit” for the application type you want to edit.
 - Step 5** To choose a different bandwidth limit value, select **Set Bandwidth Limit** and enter the amount of traffic to limit in either Megabits per second (Mbps) or kilobits per second (kbps). To specify no bandwidth limit, select **No Bandwidth Limit for Application Type**.
 - Step 6** Click **Apply**.
 - Step 7** **Submit** and **Commit Changes**.
-

Configuring Bandwidth Controls for an Application

-
- Step 1** Choose **Web Security Manager > Access Policies**.
 - Step 2** Click the link in the policies table under the Applications column for the policy group you want to edit.
 - Step 3** Expand the application type that contains the application you want to define.
 - Step 4** Click the link for the application you want to configure.
 - Step 5** Select **Monitor**, and then choose to use either the bandwidth limit defined for the application type or no limit.



Note The bandwidth limit setting is not applicable when the application is blocked or when no bandwidth limit is defined for the application type.

- Step 6** Click **Done**.
 - Step 7** **Submit** and **Commit Changes**.
-

Controlling Instant Messaging Traffic

You can block or monitor the IM traffic, and depending on the IM service, you can block particular activities (also known as application behaviors) in an IM session.

-
- Step 1** Choose **Web Security Manager > Access Policies**.
 - Step 2** Click the link in the policies table under the Applications column for the policy group you want to edit.
 - Step 3** Click **Define Applications Custom Setting**.

- Step 4** Expand the Instant Messaging application type.
 - Step 5** Click the link next to the IM application you want to configure.
 - Step 6** To block all traffic for this IM application, select **Block**.
 - Step 7** To monitor the IM application, but block particular activities within the application, select **Monitor**, and then select the application behavior to **Block**.
 - Step 8** Click **Done**.
 - Step 9** **Submit** and **Commit Changes**.
-

Viewing AVC Activity

The **Reporting > Application Visibility** page displays information about the top applications and application types used. It also displays the top applications and application types blocked.

Access Log File

The access log file records the information returned by the Application Visibility and Control engine for each transaction. The scanning verdict information section in the access logs includes the fields listed below:

Description	Custom Field in Access Logs	Custom Field in W3C Logs
Application name	%XO	x-avc-app
Application type	%Xu	x-avc-type
Application behavior	%Xb	x-avc-behavior



Prevent Loss of Sensitive Data

- [Overview of Data Security and External DLP Policies, page 13-1](#)
- [Managing Upload Requests, page 13-2](#)
- [Managing Upload Requests on an External DLP System, page 15-3](#)
- [Evaluating Data Security and External DLP Policy Group Membership, page 15-4](#)
- [Creating Data Security and External DLP Policies, page 15-5](#)
- [Managing Settings for Upload Requests, page 15-7](#)
- [Defining External DLP Systems, page 15-9](#)
- [Controlling Upload Requests Using External DLP Policies, page 15-11](#)
- [Logging, page 15-11](#)

Overview of Prevent Loss of Sensitive Data

The Web Security appliance secures your data by providing the following capabilities:

Option	Description
Cisco IronPort Data Security Filters	The Cisco IronPort Data Security Filters on the Web Security appliance evaluate data leaving the network over HTTP, HTTPS and FTP.
Third party data loss prevention (DLP) integration	The Web Security appliance integrates with leading third party content-aware DLP systems that identify and protect sensitive data. The Web Proxy uses the Internet Content Adaptation Protocol (ICAP) which allows proxy servers to offload content scanning to external systems

When the Web Proxy receives an upload request, it compares the request to the Data Security and External DLP Policy groups to determine which policy group to apply. If both types of policies are configured, it compares the request to Cisco IronPort Data Security Policies before external DLP Policies. After it assigns the request to a policy group, it compares the request to the policy group's configured control settings to determine what to do with the request. How you configure the appliance to handle upload requests depends on the policy group type.



Note

Upload requests that try to upload files with a size of zero (0) bytes are not evaluated against Cisco IronPort Data Security or External DLP Policies.

To restrict and control data that is leaving the network, you can perform the following tasks:

Task	Link to Task
Create Cisco IronPort Data Security Policies	Managing Upload Requests, page 13-2
Create External DLP Policies	Managing Upload Requests on an External DLP System, page 13-3
Create Data Security and External DLP Policies	Creating Data Security and External DLP Policies, page 15-5
Control Upload Requests using Cisco IronPort Data Security Policies	Managing Settings for Upload Requests, page 13-7
Control Upload Requests Using External DLP Policies	Controlling Upload Requests Using External DLP Policies, page 13-11

Bypassing Upload Requests Below a Minimum Size

To help reduce the number of upload requests recorded in the log files, you can define a minimum request body size, below which upload requests are not scanned by the Cisco IronPort Data Security Filters or the external DLP server.

To do this, use the following CLI commands:

- **datasecurityconfig**. Applies to the Cisco IronPort Data Security Filters.
- **externaldlpconfig**. Applies to the configured external DLP servers.

The default minimum request body size is 4 KB (4096 bytes) for both CLI commands. Valid values are 1 to 64 KB. The size you specify applies to the entire size of the upload request body.



Note

All chunk encoded uploads and all native FTP transactions are scanned by the Cisco IronPort Data Security Filters or external DLP servers when enabled. However, they can still be bypassed based on a custom URL category.

User Experience with Blocked Requests

When the Cisco IronPort Data Security Filters or an external DLP server blocks an upload request, it provides a block page that the Web Proxy sends to the end user. Not all websites display the block page to the end user. For example, some Web 2.0 websites display dynamic content using javascript instead of a static webpage and are not likely to display the block page. Users are still properly blocked from performing data security violations, but they may not always be informed of this by the website.

Managing Upload Requests

Before You Begin

- Go to **Security Services > Data Security Filters** to enable the Cisco IronPort Data Security Filters.

- Step 1 Create and configure Data Security Policy groups.** Cisco IronPort Data Security Policies use URL filtering, web reputation, and upload content information when evaluating the upload request. You configure each of these security components to determine whether or not to block the upload request.
- When the Web Proxy compares an upload request to the control settings, it evaluates the settings in order. Each control setting can be configured to perform one of the following actions for Cisco IronPort Data Security Policies:

Action	Description
Block	The Web Proxy does not permit the connection and instead displays an end user notification page explaining the reason for the block.
Allow	The Web Proxy bypasses the rest of the Data Security Policy security service scanning and then evaluates the request against the Access Policies before taking a final action. For Cisco IronPort Data Security Policies, Allow bypasses the rest of data security scanning, but does not bypass External DLP or Access Policy scanning. The final action the Web Proxy takes on the request is determined by the applicable Access Policy (or an applicable external DLP Policy that may block the request).
Monitor	The Web Proxy continues comparing the transaction to the other Data Security Policy group control settings to determine whether to block the transaction or evaluate it against the Access Policies.

For Cisco IronPort Data Security Policies, only the Block action is a final action that the Web Proxy takes on a client request. The Monitor and Allow actions are intermediary actions. In both cases, the Web Proxy evaluates the transaction against the External DLP Policies (if configured) and Access Policies. The Web Proxy determines which final action to apply based on the Access Policy group control settings (or an applicable external DLP Policy that may block the request).

Related Topics

- [Managing Upload Requests on an External DLP System, page 13-3](#)
- [Managing Settings for Upload Requests, page 15-7](#)

Managing Upload Requests on an External DLP System

To configure the Web Security appliance to handle upload requests on an external DLP system, perform the following tasks:

- Step 1** Choose **Network > External DLP Servers**. Define an external DLP system. To pass an upload request to an external DLP system for scanning, you must define at least one ICAP-compliant DLP system on the Web Security appliance.
- Step 2** **Create and configure External DLP Policy groups.** After an external DLP system is defined, you create and configure External DLP Policy groups to determine which upload requests to send to the DLP system for scanning.
- Step 3** When an upload request matches an External DLP Policy, the Web Proxy sends the upload request to the DLP system using the Internet Content Adaptation Protocol (ICAP) for scanning. The DLP system scans the request body content and returns a block or allow verdict to the Web Proxy. The allow verdict is

similar to the Allow action for Cisco IronPort Data Security Policies in that the upload request will be compared to the Access Policies. The final action the Web Proxy takes on the request is determined by the applicable Access Policy.

Related Topics

- [Controlling Upload Requests Using External DLP Policies, page 15-11](#)
- [Defining External DLP Systems, page 15-9](#)

Evaluating Data Security and External DLP Policy Group Membership

Each client request is assigned to an Identity and then is evaluated against the other policy types to determine which policy group it belongs for each type. The Web Proxy evaluates *upload requests* against the Data Security and External DLP Policies. The Web Proxy applies the configured policy control settings to a client request based on the client request's policy group membership.

Matching Client Requests to Data Security and External DLP Policy Groups

To determine the policy group that a client request matches, the Web Proxy follows a specific process for matching the group membership criteria. It considers the following factors for group membership:

- **Identity.** Each client request either matches an Identity, fails authentication and is granted guest access, or fails authentication and gets terminated.
- **Authorized users.** If the assigned Identity requires authentication, the user must be in the list of authorized users in the Data Security or External DLP Policy group to match the policy group. The list of authorized users can be any of the specified groups or users or can be guest users if the Identity allows guest access.
- **Advanced options.** You can configure several advanced options for Data Security and External DLP Policy group membership. Some options (such as proxy port and URL category) can also be defined within the Identity. When an advanced option is configured in the Identity, it is not configurable in the Data Security or External DLP Policy group level.

The information in this section gives an overview of how the Web Proxy matches upload requests to both Data Security and External DLP Policy groups.

The Web Proxy sequentially reads through each policy group in the policies table. It compares the upload request status to the membership criteria of the first policy group. If they match, the Web Proxy applies the policy settings of that policy group.

If they do not match, the Web Proxy compares the upload request to the next policy group. It continues this process until it matches the upload request to a user defined policy group. If it does not match a user defined policy group, it matches the global policy group. When the Web Proxy matches the upload request to a policy group or the global policy group, it applies the policy settings of that policy group.

Creating Data Security and External DLP Policies

You can create Data Security and External DLP Policy groups based on combinations of several criteria, such as one or more Identities or the URL category of the destination site. You must define at least one criterion for policy group membership. When you define multiple criteria, the upload request must meet all criteria to match the policy group. However, the upload request needs to match only one of the configured Identities.

-
- Step 1** Choose **Web Security Manager > Cisco IronPort Data Security** (for Defining Data Security Policy group membership) or **Web Security Manager > External Data Loss Prevention** (for Defining External DLP Policy group membership).
- Step 2** Click **Add Policy**.
- Step 3** In the Policy Name field, enter a name for the policy group, and in the Description field (optional) add a description.



Note Each policy group name must be unique and only contain alphanumeric characters or the space character.

- Step 4** In the Insert Above Policy field, choose where in the policies table to place the policy group. When configuring multiple policy groups you must specify a logical order for each group. Order your policy groups to ensure that correct matching occurs.
- Step 5** In the Identities and Users section, choose one or more Identity groups to apply to this policy group.
- Step 6** (Optional) Expand the Advanced section to define additional membership requirements.

- Step 7** To define policy group membership by any of the advanced options, click the link for the advanced option and configure the option on the page that appears.

Advanced Option	Description
Protocols	<p>Choose whether or not to define policy group membership by the protocol used in the client request. Select the protocols to include.</p> <p>“All others” means any protocol not listed above this option.</p> <p>Note When the HTTPS Proxy is enabled, only Decryption Policies apply to HTTPS transactions. You cannot define policy membership by the HTTPS protocol for Access, Routing, Outbound Malware Scanning, Data Security, or External DLP Policies.</p>
Proxy Ports	<p>Choose whether or not to define policy group membership by the proxy port used to access the Web Proxy. Enter one or more port numbers in the Proxy Ports field. Separate multiple ports with commas.</p> <p>For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port. You might want to define policy group membership on the proxy port if you have one set of clients configured to explicitly forward requests on one port, and another set of clients configured to explicitly forward requests on a different port.</p> <p>Cisco recommends only defining policy group membership by the proxy port when the appliance is deployed in explicit forward mode, or when clients explicitly forward requests to the appliance. If you define policy group membership by the proxy port when client requests are transparently redirected to the appliance, some requests might be denied.</p> <p>Note If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</p>
Subnets	<p>Choose whether or not to define policy group membership by subnet or other addresses.</p> <p>You can choose to use the addresses that may be defined with the associated Identity, or you can enter specific addresses here.</p> <p>Note If the Identity associated with this policy group defines its membership by addresses, then in this policy group you must enter addresses that are a subset of the addresses defined in the Identity. Adding addresses in the policy group further narrows down the list of transactions that match this policy group.</p>
URL Categories	<p>Choose whether or not to define policy group membership by URL categories. Select the user defined or predefined URL categories.</p> <p>Note If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</p>

Advanced Option	Description
User Agents	<p>Choose whether or not to define policy group membership by the user agent used in the client request. You can select some commonly defined browsers, or define your own using regular expressions. Choose whether this policy group should apply to the selected user agents or to any user agent that is not in the list of selected user agents.</p> <p>Note If the Identity associated with this policy group defines Identity membership by this advanced setting, the setting is not configurable at the non-Identity policy group level.</p>
User Location	<p>Choose whether or not to define policy group membership by user location, either remote or local.</p> <p>This option only appears when the Secure Mobility is enabled.</p>

Step 8 Submit your changes.

Step 9 If you are creating a Data Security Policy group, configure its control settings to define how the Web Proxy handles upload requests.

The new Data Security Policy group automatically inherits global policy group settings until you configure options for each control setting.

If you are creating an External DLP Policy group, configure its control settings to define how the Web Proxy handles upload requests.

The new External DLP Policy group automatically inherits global policy group settings until you configure custom settings.

Step 10 **Submit and Commit Changes.**

Related Topics

- [Evaluating Data Security and External DLP Policy Group Membership, page 15-4](#)
- [Matching Client Requests to Data Security and External DLP Policy Groups, page 15-4](#)
- [Managing Settings for Upload Requests, page 15-7](#)
- [Controlling Upload Requests Using External DLP Policies, page 15-11](#)

Managing Settings for Upload Requests

Each upload request is assigned to a Data Security Policy group and inherits the control settings of that policy group. The control settings of the Data Security Policy group determine whether the appliance blocks the connection or evaluates it against the Access Policies.

Configure control settings for Data Security Policy groups on the **Web Security Manager > Cisco IronPort Data Security** page.

You can configure the following settings to determine what action to take on upload requests:

Option	Link
URL Categories	URL Categories, page 13-8
Web Reputation	Web Reputation, page 13-8
Content	Content Blocking, page 13-8

After a Data Security Policy group is assigned to an upload request, the control settings for the policy group are evaluated to determine whether to block the request or evaluate it against the Access Policies.

URL Categories

AsyncOS for Web allows you to configure how the appliance handles a transaction based on the URL category of a particular request. Using a predefined category list, you can choose to monitor or block content by category. You can also create custom URL categories and choose to allow, monitor, or block traffic for a website in the custom category.

Web Reputation

The Web Reputation setting inherits the global setting. To customize web reputation filtering for a particular policy group, you can use the Web Reputation Settings pull-down menu to customize web reputation score thresholds.

Only negative and zero values can be configured for web reputation threshold settings for Cisco IronPort Data Security Policies. By definition, all positive scores are monitored.

Content Blocking

You can use the settings on the Cisco IronPort Data Security Policies > Content page to configure the Web Proxy to block data uploads based on the following file characteristics:

- **File size.** You can specify the maximum *upload* size allowed. All uploads with sizes equal to or greater than the specified maximum are blocked. You can specify different maximum file sizes for HTTP/HTTPS and native FTP requests.

When the upload request size is greater than both the maximum upload size and the maximum scan size (configured in the “DVS Engine Object Scanning Limits” field on Security Services > Anti-Malware page), the upload request is still blocked, but the entry in the data security logs does not record the file name and content type. The entry in the access logs is unchanged.

- **File type.** You can block predefined file types or custom MIME types you enter. When you block a predefined file type, you can block all files of that type or files greater than a specified size. When you block a file type by size, the maximum file size you can specify is the same as the value for the “DVS Engine Object Scanning Limits” field on Security Services > Anti-Malware page. By default, that value is 32 MB.

Cisco IronPort Data Security Filters do not inspect the contents of archived files when blocking by file type. Archived files can be blocked by its file type or file name, not according to its contents.

**Note**

For some groups of MIME types, blocking one type blocks all MIME types in the group. For example, blocking application/x-java-applet blocks all java MIME types, such as application/java and application/javascript.

- **File name.** You can block files with specified names. You can use text as a literal string or a regular expression for specifying file names to block.

**Note**

Only enter file names with 8-bit ASCII characters. The Web Proxy only matches file names with 8-bit ASCII characters.

Defining External DLP Systems

The Web Security appliance can integrate with multiple external DLP servers from the same vendor by defining multiple DLP servers in the appliance. You can define the load balancing technique the Web Proxy uses when contacting the DLP systems. This is useful when you define multiple DLP systems.

**Note**

Verify the external DLP server does not send the Web Proxy modified content. AsyncOS for Web only supports the ability to block or allow upload requests. It does not support uploading content modified by an external DLP server.

Configuring External DLP Servers

Step 1 Choose **Network > External DLP Servers**.

Step 2 Click **Edit Settings**.

Setting	Description
External DLP Servers	<p>Enter the following information to access an ICAP compliant DLP system:</p> <ul style="list-style-type: none"> • Server address and port. The hostname or IP address and TCP port for accessing the DLP system. • Reconnection attempts. The number of times the Web Proxy tries to connect to the DLP system before failing. • DLP Service URL. The ICAP query URL specific to the particular DLP server. The Web Proxy includes what you enter here in the ICAP request it sends to the external DLP server. The URL must start with the ICAP protocol: icap://
Load Balancing	<p>If multiple DLP servers are defined, select which load balancing technique the Web Proxy uses to distribute upload requests to different DLP servers. You can choose the following load balancing techniques:</p> <ul style="list-style-type: none"> • None (failover). The Web Proxy directs upload requests to one DLP server. It tries to connect to the DLP servers in the order they are listed. If one DLP server cannot be reached, the Web Proxy attempts to connect to the next one in the list. • Fewest connections. The Web Proxy keeps track of how many active requests are with the different DLP servers and it directs the upload request to the DLP server currently servicing the fewest number of connections. • Hash based. The Web Proxy uses a hash function to distribute requests to the DLP servers. The hash function uses the proxy ID and URL as inputs so that requests for the same URL are always directed to the same DLP server. • Round robin. The Web Proxy cycles upload requests equally among all DLP servers in the listed order.
Service Request Timeout	<p>Enter how long the Web Proxy waits for a response from the DLP server. When this time is exceeded, the ICAP request has failed and the upload request is either blocked or allowed, depending on the Failure Handling setting.</p> <p>Default is 60 seconds.</p>
Maximum Simultaneous Connections	<p>Specifies the maximum number of simultaneous ICAP request connections from the Web Security appliance to each configured external DLP server. The Failure Handling setting on this page applies to any request which exceeds this limit.</p> <p>Default is 25.</p>
Failure Handling	<p>Choose whether upload requests are blocked or allowed (passed to Access Policies for evaluation) when the DLP server fails to provide a timely response.</p> <p>Default is allow (“Permit all data transfers to proceed without scanning”).</p>

Step 3 (Optional) You can add another DLP server by clicking **Add Row** and entering the DLP Server information in the new fields provided.

- Step 4** You can test the connection between the Web Security appliance and the defined external DLP server(s) by clicking **Start Test**.
- Step 5** **Submit** and **Commit Changes**.
-

Controlling Upload Requests Using External DLP Policies

Once the Web Proxy receives the upload request headers, it has the information necessary to decide if the request should go to the external DLP system for scanning. The DLP system scans the request and returns a verdict to the Web Proxy, either block or monitor (evaluate the request against the Access Policies).

-
- Step 1** Choose **Web Security Manager > External Data Loss Prevention**.
- Step 2** Click the link under the Destinations column for the policy group you want to configure.
- Step 3** Under the **Edit Destination Settings** section, choose “**Define Destinations Scanning Custom Settings**”.
- Step 4** In the Destination to scan section, choose one of the following options:
- **Do not scan any uploads.** No upload requests are sent to the configured DLP system(s) for scanning. All upload requests are evaluated against the Access Policies.
 - **Scan all uploads.** All upload requests are sent to the configured DLP system(s) for scanning. The upload request is blocked or evaluated against the Access Policies depending on the DLP system scanning verdict.
 - **Scan uploads to specified custom URL categories only.** Upload requests that fall in specific custom URL categories are sent to the configured DLP system for scanning. The upload request is blocked or evaluated against the Access Policies depending on the DLP system scanning verdict. Click **Edit custom categories list** to select the URL categories to scan.
- Step 5** **Submit** and **Commit Changes**.
-

Logging

The access logs indicate whether or not an upload request was scanned by either the Cisco IronPort Data Security Filters or an external DLP server. The access log entries include a field for the Cisco IronPort Data Security scan verdict and another field for the External DLP scan verdict based.

In addition to the access logs, the Web Security appliance provides the following log file types to troubleshoot Cisco IronPort Data Security and External DLP Policies:

- **Data Security Logs.** Records client history for upload requests that are evaluated by the Cisco IronPort Data Security Filters.
- **Data Security Module Logs.** Records messages related to the Cisco IronPort Data Security Filters.
- **Default Proxy Logs.** In addition recording errors related to the Web Proxy, the default proxy logs include messages related to connecting to external DLP servers. This allows you to troubleshoot connectivity or integration problems with external DLP servers.

The following text illustrates a sample Data Security Log entry:

```
Mon Mar 30 03:02:13 2009 Info: 303 10.1.1.1 - -
<<bar,text/plain,5120><foo,text/plain,5120>>
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting ns server.com nc
```

Field Value	Description
Mon Mar 30 03:02:13 2009 Info:	Timestamp and trace level
303	Transaction ID
10.1.1.1	Source IP address
-	User name
-	Authorized group names
<<bar,text/plain,5120><foo,text/plain,5120>>	File name, file type, file size for each file uploaded at once Note This field does not include text/plain files that are less than the configured minimum request body size, the default of which is 4096 bytes.
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting	Cisco IronPort Data Security Policy and action
ns	Web reputation score
server.com	Outgoing URL
nc	URL category


Note

To learn when data transfer, such as a POST request, to a site was blocked by the external DLP server, search for the IP address or hostname of the DLP server in the access logs.



Notify End-Users of Proxy Actions

- [End-User Notifications Overview, page 16-1](#)
- [Related Topics, page 16-4](#)
- [General Notification Settings, page 16-3](#)
- [On-Box End-User Notification Pages, page 16-4](#)
- [Off-Box End-User Notification Pages, page 16-8](#)
- [End-User Acknowledgment Page, page 16-10](#)
- [Access HTTPS and FTP Sites with the End-User Acknowledgment Page, page 16-12](#)
- [Configuring FTP Notification Messages, page 16-13](#)
- [Custom Text in Notification Pages, page 16-13](#)
- [Notification Page Types, page 16-15](#)

End-User Notifications Overview

When a policy blocks a user from a website, you can configure the appliance to notify the user why it blocked the URL request. These pages are called end-user notification pages.

You can configure the following types of notification pages and settings:

Option	Description	Further information
General notification settings.	You can configure the language used in on-box end-user notification pages for both HTTP and FTP. You can also configure a logo to use for on-box end-user notification pages for HTTP requests.	Configuring General Settings for Notification Pages, page 16-4.
On-box end-user notification pages.	Predefined notification pages that are customizable, are displayed depending on the reason for blocking the URL request.	Configuring On-Box End-User Notification Pages, page 16-4. Editing On-Box End-User Notification Pages, page 16-5

Option	Description	Further information
Off-box end-user notification pages.	The Web Proxy can be configured to redirect all HTTP end-user notification pages to a specific URL. The Web Proxy includes parameters in the redirected URL that explain the reasons for the block so the server in the redirected URL can customize the page it displays.	Redirecting End-User Notification Pages to a Custom URL, page 16-9.
End-user acknowledgment page.	The Web Proxy can be configured to inform users that it is filtering and monitoring their web activity. An end-user acknowledgment page is displayed when a user first accesses a browser after a certain period of time.	Configuring the End-User Acknowledgment Page, page 16-11
End-user URL filtering warning page.	The Web Proxy can be configured to warn users that a site does not meet the organization's acceptable use policies and allow them to continue if they choose. An end-user URL filtering warning page is displayed when a user first accesses a website in a particular URL category after a certain period of time. You can also configure the warning page when a user accesses adult content when the site content ratings feature is enabled.	Configuring the End-User URL Filtering Warning Page, page 16-12
FTP notification messages.	The FTP Proxy displays a different, predefined notification messages depending on the reason for blocking a native FTP transaction. You can customize these pages with a custom message.	Configuring FTP Notification Messages, page 16-13.

Notification Best Practices

- [Editing On-Box End-User Notification Pages, page 16-5](#)
- [End-User Notification Page Parameters, page 16-8](#)
- [Redirecting End-User Notification Pages to a Custom URL, page 16-9](#)
- [Configuring the End-User Acknowledgment Page, page 16-11](#)

Editing On-Box End-User Notification Pages

- Each customized on-box end-user notification page file must be a valid HTML file. For a list of HTML tags you can include, see [Supported HTML Tags in Notification Pages, page 16-13](#).
- The customized on-box end-user notification page file names must exactly match the file names shipped with the Web Security appliance.
- Do not include any links to URLs in the HTML files. Any link included in the notification pages are subject to the access control rules defined in the Access Policies and users might end up in a recursive loop.
- If the configuration\eun directory does not contain a particular file with the required name, then the appliance displays the standard on-box end-user notification page.
- For new customized on-box end-user notification pages to go into effect, you must first upload the customized files to the appliance and then enable the customized files using the `advancedproxyconfig > EUN CLI` command.

About General Settings for Notification Pages

You can configure the following general settings:

- **Language.** You can configure a different language for HTTP and FTP end-user notification pages. The HTTP language setting applies to all HTTP notification pages (acknowledgment, on-box end-user, customized end-user, and end-user URL filtering warning), and the FTP language applies to all FTP notification messages.
- **Logo.** You can configure a logo for HTTP end-user notification pages only. The logo setting applies to all HTTP notification pages served over IPv4. AsyncOS does not support images over IPv6.

Configuring General Settings for Notification Pages

-
- Step 1** Security Services > End-User Notification.
 - Step 2** Click **Edit Settings**.
 - Step 3** In the General Settings section, select the language the Web Proxy should use when displaying HTTP notification pages.
 - Step 4** Choose whether or not to use a logo on each notification page. You can specify the Cisco logo or any graphic file referenced at the URL you enter in the Use Custom Logo field.
 - Step 5** **Submit** and **Commit Changes**.
-

Related Topics

- [Custom Text and Logos: Authentication, and End-User Acknowledgment Pages, page 16-14](#)

On-Box End-User Notification Pages

When enabled, the Web Proxy displays a different page depending on the reason why it blocked the original page. each page is customizable to make them specific to your organization.

Configuring On-Box End-User Notification Pages

Before you begin

- Review [Supported HTML Tags in Notification Pages, page 16-13](#)

-
- Step 1** Security Services > End-User Notification.
 - Step 2** Click **Edit Settings**.
 - Step 3** From the Notification Type field, choose Use On Box End User Notification.

Step 4 Configure the on-box end-user notification page settings.

Setting	Description
Custom Message	Include any additional text required on each notification page. When you enter a custom message, AsyncOS places the message before the last sentence on the notification page which includes the contact information.
Contact Information	Customize the contact information listed on each notification page. AsyncOS displays the contact information sentence as the last sentence on a page, before providing notification codes that users can provide to the network administrator.
End-User Misclassification Reporting	When enabled, users can report misclassified URLs to Cisco. An additional button appears on the on-box end-user notification pages for sites blocked due to suspected malware or URL filters. This button allows the user to report when they believe the page has been misclassified. It does not appear for pages blocked due to other policy settings.

Step 5 (Optional) Click **Preview Notification Page Customization** link to view the current end-user notification page in a separate browser window.



Note If the end-user notification pages have been edited this preview functionality is not available.

Step 6 **Submit and Commit Changes.**

Editing On-Box End-User Notification Pages

Each on-box end-user notification page is stored on the Web Security appliance as an HTML file. You can edit the content of these HTML pages to include additional text or to edit the overall look and feel of each page.

You can use variables in the HTML files to display specific information to the user. You can also turn each variable into a conditional variable to create if-then statements. For more information, see [Use Variables in Customized On-Box End-User Notification Pages, page 16-7](#).

Table below describes the variables you can include in customized end-user notification pages.

Variable	Description	Always Evaluates to TRUE if Used as Conditional Variable
%a	Authentication realm for FTP	No
%A	ARP address	Yes
%b	User-agent name	No
%B	Blocking reason, such as BLOCK-SRC or BLOCK-TYPE	No
%c	Error page contact person	Yes
%C	Entire Set-Cookie: header line, or empty string	No
%d	Client IP address	Yes

Variable	Description	Always Evaluates to TRUE if Used as Conditional Variable
%D	User name	No
%e	Error page email address	Yes
%E	The error page logo URL	No
%f	User feedback section	No
%F	The URL for user feedback	No
%g	The web category name, if available	Yes
%G	Maximum file size allowed in MB	No
%h	The hostname of the proxy	Yes
%H	The server name of the URL	Yes
%i	Transaction ID as a hexadecimal number	Yes
%I	Management IP Address	Yes
%j	URL category warning page custom text	No
%k	Redirection link for the end-user acknowledgment page and end-user URL filtering warning page	No
%K	Response file type	No
%l	WWW-Authenticate: header line	No
%L	Proxy-Authenticate: header line	No
%M	The Method of the request, such as “GET” or “POST”	Yes
%n	Malware category name, if available	No
%N	Malware threat name, if available	No
%o	Web reputation threat type, if available	No
%O	Web reputation threat reason, if available	No
%p	String for the Proxy-Connection HTTP header	Yes
%P	Protocol	Yes
%q	Identity policy group name	Yes
%Q	Policy group name for non-Identity policies	Yes
%r	Redirect URL	No
%R	Re-authentication is offered. This variable outputs an empty string when false and a space when true, so it is not useful to use it alone. Instead, use it as condition variable.	No
%S	The signature of the proxy	No, always evaluates to FALSE
%t	Timestamp in Unix seconds plus milliseconds	Yes
%T	The date	Yes
%u	The URI part of the URL (the URL excluding the server name)	Yes
%U	The full URL of the request	Yes
%v	HTTP protocol version	Yes

Variable	Description	Always Evaluates to TRUE if Used as Conditional Variable
%W	Management WebUI port	Yes
%X	Extended blocking code. This is a 16-byte base64 value that encodes the most of the web reputation and anti-malware information logged in the access log, such as the ACL decision tag and WBRs score.	Yes
%Y	Administrator custom text string, if set, else empty	No
%y	End-user acknowledgment page custom text	Yes
%z	Web reputation score	Yes
%Z	DLP meta data	Yes
%%	Prints the percent symbol (%) in the notification page	N/A

To edit the on-box end-user notification pages:

-
- Step 1** Use an FTP client to connect to the Web Security appliance.
 - Step 2** Navigate to the `configuration\eun` directory.
 - Step 3** Download the language directory files for the on-box end-user notification pages you want to edit.
 - Step 4** On your local machine, use a text or HTML editor to edit each HTML file for the on-box end-user notification pages.
 - Step 5** Use the FTP client to upload the customized HTML files to the same directory from which you downloaded them in step 3.
 - Step 6** Open an SSH client and connect to the Web Security appliance.
 - Step 7** Run the `advancedproxyconfig > EUN` CLI command.
 - Step 8** Type `2` to use the custom end-user notification pages.



Note If the custom end-user notification pages option is currently enabled when you update the HTML files, you must type `1` to refresh the custom end-user notification pages. If you do not do this, the new files do not take effect until the Web Proxy restarts.

- Step 9** Commit your change, and close the SSH client.
-

Use Variables in Customized On-Box End-User Notification Pages

When editing on-box end-user notification pages, you can include conditional variables to create if-then statements to take different actions depending on the current state.

The table describes the different conditional variable formats.

Conditional Variable Format	Description
<code>??V</code>	This conditional variable evaluates to TRUE if the output of variable <code>%V</code> is not empty.
<code>%!V</code>	Represents the following condition: else Use this with the <code>??V</code> conditional variable.
<code>##V</code>	Represents the following condition: endif Use this with the <code>??V</code> conditional variable.

For example, the following text is some HTML code that uses `%R` as a conditional variable to check if re-authentication is offered, and uses `%r` as a regular variable to provide the re-authentication URL.

```

%?R
<div align="left">
  <form name="ReauthInput" action="%r" method="GET">
    <input name="Reauth" type="button" onClick="document.location='%r' "
id="Reauth" value="Login as different user...">
  </form>
</div>
%#R

```

Any variable included in [Editing On-Box End-User Notification Pages](#) can be used as a conditional variable. However, the best variables to use in conditional statements are the ones that relate to the *client request* instead of the server response, and the variables that may or may not evaluate to TRUE instead of the variables that always evaluate to TRUE.

Off-Box End-User Notification Pages

You can define notification pages outside the Web Security appliance by redirecting all notification pages to a custom URL you specify. By default, AsyncOS redirects all blocked websites to the URL regardless of the reason why it blocked the original page. However, AsyncOS also passes parameters as a query string appended to the redirect URL so you can ensure that the user sees a unique page explaining the reason for the block. For more information on the included parameters, see [End-User Notification Page Parameters, page 16-8](#).

When you want the user to view a different page for each reason for a blocked website, construct a CGI script on the web server that can parse the query string in the redirect URL. Then the server can perform a second redirect to an appropriate page.

End-User Notification Page Parameters

AsyncOS passes the parameters to the web server as standard URL Parameters in the HTTP GET request. It uses the following format:

```
<notification_page_url>?param1=value1&param2=value2
```

The table describes the parameters AsyncOS includes in the query string.

Parameter Name	Description
Time	Date and time of the transaction.
ID	Transaction ID.
Client_IP	IP address of the client.
User	Username of the client making the request, if available.
Site	Hostname of the destination in the HTTP request.
URI	URL path specified in the HTTP request.
Status_Code	HTTP status code for the request.
Decision_Tag	ACL decision tag as defined in the Access log entry that indicates how the DVS engine handled the transaction.
URL_Cat	URL category that the URL filtering engine assigned to the transaction request. Note: AsyncOS for Web sends the entire URL category name for both predefined and user defined URL categories. It performs URL encoding on the category name, so spaces are written as "%20".
WBRS	WBRS score that the Web Reputation Filters assigned to the URL in the request.
DVS_Verdict	Malware category that the DVS engine assigns to the transaction.
DVS_ThreatName	The name of the malware found by the DVS engine.
Reauth_URL	A URL that users can click to authenticate again if the user is blocked from a website due to a restrictive URL filtering policy. Use this parameter when the "Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction" global authentication setting is enabled and the user is blocked from a website due to a blocked URL category. To use this parameter, make sure the CGI script performs the following steps: 1. Get the value of <code>Reauth_Url</code> parameter. 2. URL-decode the value. 3. Base64 decode the value and get the actual re-authentication URL. 4. Include the decoded URL on the end-user notification page in some way, either as a link or button, along with instructions for users informing them they can click the link and enter new authentication credentials that allow greater access.



Note

AsyncOS always includes all parameters in each redirected URL. If no value exists for a particular parameter, AsyncOS passes a hyphen (-).

Redirecting End-User Notification Pages to a Custom URL

- Step 1** Security Services > End-User Notification.
- Step 2** Click **Edit Settings**.
- Step 3** Choose **Redirect to Custom URL**.

- Step 4** In the Notification Page URL field, enter the URL to which you want to redirect blocked websites.
- Step 5** (Optional) Click **Preview Custom URL** link.
- Step 6** **Submit** and **Commit Changes**.

End-User Acknowledgment Page

You can configure the Web Security appliance to inform users that it is filtering and monitoring their web activity. When configured the appliance displays an end-user acknowledgment page for every user accessing the web using HTTP or HTTPS. It displays the end-user acknowledgment page when a user tries to access a website for the first time, or after a configured time interval.

The Web Proxy tracks users by username if authentication has made a username available. If no user name is available, you can choose how to track users, either by IP address or web browser session cookie.



Note

Native FTP transactions are exempt from the end-user acknowledgment page.

The table describes the settings you can configure when you enable the end-user acknowledgment page.

Setting	Description
Time Between Acknowledgements	<p>The Time Between Acknowledgments determines how often the Web Proxy displays the end-user acknowledgment page for each user. This setting applies to users tracked by username and users tracked by IP address or session cookie. You can specify any value from 30 to 2678400 seconds (one month). Default is one day (86400 seconds).</p> <p>When the Time Between Acknowledgments changes and is committed, the Web Proxy uses the new value even for users who have already acknowledged the Web Proxy.</p>
Inactivity Timeout	<p>The Inactivity Timeout determines how long a user tracked and acknowledged by IP address or session cookie (unauthenticated users only) can be idle before the user is no longer considered acknowledged. You can specify any value from 30 to 2678400 seconds (one month). Default is four hours (14400 seconds).</p>

Setting	Description
Surrogate Type	<p>Determines which method the Web Proxy uses to track the user:</p> <ul style="list-style-type: none"> • IP Address. The Web Proxy allows the user at that IP address to use any web browser or non-browser HTTP process to access the web once the user clicks the link on the end-user acknowledgment page. Tracking the user by IP address allows the user to access the web until the Web Proxy displays a new end-user acknowledgment page due to inactivity or the configured time interval for new acknowledgments. Unlike tracking by a session cookie, tracking by IP address allows the user to open up multiple web browser applications and not have to agree to the end-user acknowledgment unless the configured time interval has expired. <p>Note When IP address is configured and the user is authenticated, the Web Proxy tracks users by username instead of IP address.</p> <ul style="list-style-type: none"> • Session Cookie. The Web Proxy sends the user's web browser a cookie when the user clicks the link on the end-user acknowledgment page and uses the cookie to track their session. Users can continue to access the web using their web browser until the Time Between Acknowledgments value expires, they have been inactive longer than the allotted time, or they close their web browser. <p>If the user using a non-browser HTTP client application, they must be able to click the link on the end-user acknowledgment page to access the web. If the user opens a second web browser application, the user must go through the end-user acknowledgment process again in order for the Web Proxy to send a session cookie to the second web browser.</p> <p>Note Using a session cookie to track users when the client accesses HTTPS sites or FTP servers using FTP over HTTP is not supported.</p>
Custom message	<p>Customize the text that appears on every end-user acknowledgment page. You can include some simple HTML tags to format the text.</p> <p>Note You can only include a custom message when you configure the end-user acknowledgment page in the web interface, versus the CLI.</p>

Configuring the End-User Acknowledgment Page

You can enable and configure the end-user acknowledgment page in the web interface or the command line interface. When you configure the end-user acknowledgment page in the web interface, you can include a custom message that appears on each page.

In the CLI, use `advancedproxyconfig > eun`.

-
- Step 1** Security Services > End-User Notification.
 - Step 2** Click **Edit Settings**.
 - Step 3** Enable the “**Require end-user to click through acknowledgment page**” field.
 - Step 4** In the Time Between Acknowledgments field, enter the time interval the appliance uses between displaying the end-user acknowledgment page.

You can specify any value from 30 to 2678400 seconds (one month). Default is 1 day (86400 seconds). You can enter the value in seconds, minutes, or days. Use 's' for seconds, 'm' for minutes, and 'd' for days.

- Step 5** In the Inactivity Timeout field, enter the maximum IP address idle timeout.
- You can specify any value from 30 to 2678400 seconds (one month). Default is four hours (14400 seconds). You can enter the value in seconds, minutes, or days. Use 's' for seconds, 'm' for minutes, and 'd' for days.
- Step 6** Select the Surrogate Type.
- Step 7** In the Custom Message field, enter text you want to appear on every end-user acknowledgment page.
- Step 8** (Optional) Click **Preview Acknowledgment Page Customization** to view the current end-user acknowledgment page in a separate browser window.
- Step 9** **Submit** and **Commit Changes**.
-

Related Topics

- [Custom Text and Logos: Authentication, and End-User Acknowledgment Pages, page 16-14](#)
- [Supported HTML Tags in Notification Pages, page 16-13](#)

Access HTTPS and FTP Sites with the End-User Acknowledgment Page

The end-user acknowledgment page works because it displays an HTML page to the end user that forces them to click an acceptable use policy agreement. After users click the link, the Web Proxy redirects clients to the originally requested website. It keeps track of when users accepted the end-user acknowledgment page using a surrogate (either by IP address or web browser session cookie) if no username is available for the user.

- **HTTPS.** The Web Proxy tracks whether the user has acknowledged the end-user acknowledgment page with a cookie, but it cannot obtain the cookie unless it decrypts the transaction. You can choose to either bypass (pass through) or drop HTTPS requests when the end-user acknowledgment page is enabled and tracks users using session cookies. Do this using the `advancedproxyconfig > EUN CLI` command, and choose bypass for the “Action to be taken for HTTPS requests with Session based EUA (“bypass” or “drop”).” command.
- **FTP over HTTP.** Web browsers never send cookies for FTP over HTTP transactions, so the Web Proxy cannot obtain the cookie. To work around this, you can exempt FTP over HTTP transactions from requiring the end-user acknowledgment page. Do this by creating a custom URL category using “ftp://” as the regular expression (without the quotes) and defining an Identity policy that exempts users from the end-user acknowledgment page for this custom URL category.

Configuring the End-User URL Filtering Warning Page

-
- Step 1** **Security Services > End-User Notification.**
- Step 2** Click **Edit Settings**.
- Step 3** Scroll down to the End-User URL Filtering Warning Page section.

- Step 4** In the Time Between Warning field, enter the time interval the Web Proxy uses between displaying the end-user URL filtering warning page for each URL category per user.
- You can specify any value from 30 to 2678400 seconds (one month). Default is 1 hour (3600 seconds). You can enter the value in seconds, minutes, or days. Use 's' for seconds, 'm' for minutes, and 'd' for days.
- Step 5** In the Custom Message field, enter text you want to appear on every end-user URL filtering warning page.
- Step 6** (Optional) Click **Preview URL Category Warning Page Customization** to view the current end-user URL filtering warning page in a separate browser window.
- Step 7** **Submit and Commit Changes.**
-

Related Topics

- [Supported HTML Tags in Notification Pages, page 16-13](#)

Configuring FTP Notification Messages

The FTP Proxy displays a predefined notification message to native FTP clients when the FTP Proxy cannot establish a connection with the FTP server for any reason, such as an error with FTP Proxy authentication or a bad reputation for the server domain name.

-
- Step 1** **Security Services > End-User Notification.**
- Step 2** Click **Edit Settings.**
- Step 3** Scroll down to the Native FTP section.
- Step 4** In the Language field, select the language to use when displaying native FTP notification messages.
- Step 5** In the Custom Message field, enter the text you want to display in every native FTP notification message.
- Step 6** **Submit and Commit Changes.**
-

Custom Text in Notification Pages

The following sections apply to custom text entered for on-box end-user notification and end-user acknowledgment pages.

Supported HTML Tags in Notification Pages

You can format the text in on-box end-user notification and end-user acknowledgment pages using some HTML tags. Tags must be in lower case and follow standard HTML syntax (closing tags, etc.).

You can use the following HTML tags.

- `<a>`
- ``

- ``
- `<big></big>`
- `
`
- `<code></code>`
- ``
- `<i></i>`
- `<small></small>`
- ``

For example, you can make some text italic:

```
Please acknowledge the following statements <i>before</i> accessing the Internet.
```

With the `` tag, you can use any CSS style to format text. For example, you can make some text red:

```
<span style="color: red">Warning:</span> You must acknowledge the following statements
<i>before</i> accessing the Internet.
```

Custom Text and Logos: Authentication, and End-User Acknowledgment Pages

All combinations of URL paths and domain names in embedded links within custom text and the custom logo in on-box end-user notification, end-user acknowledgment, and end-user URL filtering warning pages are exempted from the following:

- User authentication
- End-user acknowledgment
- All scanning, such as malware scanning and web reputation scoring

For example, if the following URLs are embedded in custom text:

```
http://www.example.com/index.html
```

```
http://www.mycompany.com/logo.jpg
```

Then all of the following URLs will also be treated as exempt from all scanning:

```
http://www.example.com/index.html
```

```
http://www.mycompany.com/logo.jpg
```

```
http://www.example.com/logo.jpg
```

```
http://www.mycompany.com/index.html
```

Also, where an embedded URL is of the form: `<protocol>://<domain-name>/<directory path>/` then all sub-files and sub-directories under that directory path on the host will also be exempted from all scanning.

For example, if the following URL is embedded: `http://www.example.com/gallery2/` URLs such as `http://www.example.com/gallery2/main.php` will also be treated as exempt.

This allows administrators to create a more sophisticated page with embedded content so long as the embedded content is relative to the initial URL. However, administrators should also take care when deciding which paths to include as links and custom logos.

Notification Page Types

By default, the Web Proxy displays a notification page informing users they were blocked and the reason for the block.

Most notification pages display a different set of codes that may help administrators or Cisco Customer Support troubleshoot any potential problem. Some codes are for Cisco internal use only. The different codes that might appear in the notification pages are the same as the variables you can include in customized notification pages, as shown in [Editing On-Box End-User Notification Pages](#).

The table describes the different notification pages users might encounter.

File Name and Notification Title	Notification Description	Notification Text
ERR_ACCEPTED Feedback Accepted, Thank You	Notification page that is displayed after the users uses the “Report Misclassification” option.	The misclassification report has been sent. Thank you for your feedback.
ERR_ADAPTIVE_SECURITY Policy: General	Block page that is displayed when the user is blocked due to the Adaptive Scanning feature.	Based on your organization’s security policies, this web site <URL> has been blocked because its content has been determined to be a security risk.
ERR_ADULT_CONTENT Policy Acknowledgment	The warning page that is displayed when the end-user accesses a page that is classified as adult content. Users can click an acknowledgment link to continue to the originally requested site.	You are trying to visit a web page whose content are rated as explicit or adult. By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content. Data about your browsing behavior may be monitored and recorded. You will be periodically asked to acknowledge this statement for continued access to this kind of web page. Click here to accept this statement and access the Internet.
ERR_AVC Policy: Application Controls	Block page that is displayed when the user is blocked due to the Application Visibility and Control engine.	Based on your organization’s access policies, access to application %1 of type %2 has been blocked.
ERR_BAD_REQUEST Bad Request	Error page that results from an invalid transaction request.	The system cannot process this request. A non-standard browser may have generated an invalid HTTP request. If you are using a standard browser, please retry the request.
ERR_BLOCK_DEST Policy: Destination	Block page that is displayed when the user tries to access a blocked website address.	Based on your organization’s Access Policies, access to this web site <URL> has been blocked.

File Name and Notification Title	Notification Description	Notification Text
ERR_BROWSER Security: Browser	Block page that is displayed when the transaction request comes from an application that has been identified to be compromised by malware or spyware.	Based on your organization's Access Policies, requests from your computer have been blocked because it has been determined to be a security threat to the organization's network. Your browser may have been compromised by a malware/spyware agent identified as " <i><malware name></i> ". Please contact <i><contact name></i> <i><email address></i> and provide the codes shown below. If you are using a non-standard browser and believe it has been misclassified, use the button below to report this misclassification.
ERR_BROWSER_CUSTOM Policy: Browser	Block page that is displayed when the transaction request comes from a blocked user agent.	Based on your organization's Access Policies, requests from your browser have been blocked. This browser " <i><browser type></i> " is not permitted due to potential security risks.
ERR_CERT_INVALID Invalid Certificate	Block page that is displayed when the requested HTTPS site uses an invalid certificate.	A secure session cannot be established because the site <i><hostname></i> provided an invalid certificate.
ERR_CONTINUE_UNACKNOWLEDGED Policy Acknowledgment	Warning page that is displayed when the user requests a site that is in a custom URL category that is assigned the Warn action. Users can click an acknowledgment link to continue to the originally requested site.	You are trying to visit a web page that falls under the URL Category <i><URL category></i> . By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content. Data about your browsing behavior may be monitored and recorded. You will be periodically asked to acknowledge this statement for continued access to this kind of web page. Click here to accept this statement and access the Internet.
ERR_DNS_FAIL DNS Failure	Error page that is displayed when the requested URL contains an invalid domain name.	The hostname resolution (DNS lookup) for this hostname <i><hostname></i> has failed. The Internet address may be misspelled or obsolete, the host <i><hostname></i> may be temporarily unavailable, or the DNS server may be unresponsive. Please check the spelling of the Internet address entered. If it is correct, try this request later.
ERR_EXPECTATION_FAILED Expectation Failed	Error page that is displayed when the transaction request triggers the HTTP 417 "Expectation Failed" response.	The system cannot process the request for this site <i><URL></i> . A non-standard browser may have generated an invalid HTTP request. If using a standard browser, please retry the request.

File Name and Notification Title	Notification Description	Notification Text
ERR_FILE_SIZE Policy: File Size	Block page that is displayed when the requested file is larger than the allowed maximum file size.	Based on your organization's Access Policies, access to this web site or download <URL> has been blocked because the download size exceeds the allowed limit.
ERR_FILE_TYPE Policy: File Type	Block page that is displayed when the requested file is a blocked file type.	Based on your organization's Access Policies, access to this web site or download <URL> has been blocked because the file type "<file type>" is not allowed.
ERR_FILTER_FAILURE Filter Failure	Error page that is displayed when the URL filtering engine is temporarily unable to deliver a URL filtering response and the "Default Action for Unreachable Service" option is set to Block.	The request for page <URL> has been denied because an internal server is currently unreachable or overloaded. Please retry the request later.
ERR_FOUND Found	Internal redirection page for some errors.	The page <URL> is being redirected to <redirected URL>.
ERR_FTP_ABORTED FTP Aborted	Error page that is displayed when the FTP over HTTP transaction request triggers the HTTP 416 "Requested Range Not Satisfiable" response.	The request for the file <URL> did not succeed. The FTP server <hostname> unexpectedly terminated the connection. Please retry the request later.
ERR_FTP_AUTH_REQUIRED FTP Authorization Required	Error page that is displayed when the FTP over HTTP transaction request triggers the FTP 530 "Not Logged In" response.	Authentication is required by the FTP server <hostname>. A valid user ID and password must be entered when prompted. In some cases, the FTP server may limit the number of anonymous connections. If you usually connect to this server as an anonymous user, please try again later.
ERR_FTP_CONNECTION_FAILED FTP Connection Failed	Error page that is displayed when the FTP over HTTP transaction request triggers the FTP 425 "Can't open data connection" response.	The system cannot communicate with the FTP server <hostname>. The FTP server may be temporarily or permanently down, or may be unreachable because of network problems. Please check the spelling of the address entered. If it is correct, try this request later.
ERR_FTP_FORBIDDEN FTP Forbidden	Error page that is displayed when the FTP over HTTP transaction request is for an object the user is not allowed to access.	Access was denied by the FTP server <hostname>. Your user ID does not have permission to access this document.
ERR_FTP_NOT_FOUND FTP Not Found	Error page that is displayed when the FTP over HTTP transaction request is for an object that does not exist on the server.	The file <URL> could not be found. The address is either incorrect or obsolete.
ERR_FTP_SERVER_ERROR FTP Server Error	Error page that is displayed for FTP over HTTP transactions that try to access a server that does support FTP. The server usually returns the HTTP 501 "Not Implemented" response.	The system cannot communicate with the FTP server <hostname>. The FTP server may be temporarily or permanently down, or may not provide this service. Please confirm that this is a valid address. If it is correct, try this request later.

File Name and Notification Title	Notification Description	Notification Text
ERR_FTP_SERVICE_UNAVAIL FTP Service Unavailable	Error page that is displayed for FTP over HTTP transactions that try to access an FTP server that is unavailable.	The system cannot communicate with the FTP server <hostname>. The FTP server may be busy, may be permanently down, or may not provide this service. Please confirm that this is a valid address. If it is correct, try this request later.
ERR_GATEWAY_TIMEOUT Gateway Timeout	Error page that is displayed when the requested server has not responded in a timely manner.	The system cannot communicate with the external server <hostname>. The Internet server may be busy, may be permanently down, or may be unreachable because of network problems. Please check the spelling of the Internet address entered. If it is correct, try this request later.
ERR_IDS_ACCESS_FORBIDDEN IDS Access Forbidden	Block page that is displayed when the user tries to upload a file that is blocked due to a configured Cisco Data Security Policy.	Based on your organization's data transfer policies, your upload request has been blocked. File details: <file details>
ERR_INTERNAL_ERROR Internal Error	Error page that is displayed when there is an internal error.	Internal system error when processing the request for the page <URL>. Please retry this request. If this condition persists, please contact <contact name> <email address> and provide the code shown below.
ERR_MALWARE_SPECIFIC Security: Malware Detected	Block page that is displayed when malware is detected when downloading a file.	Based on your organization's Access Policies, this web site <URL> has been blocked because it has been determined to be a security threat to your computer or the organization's network. Malware <malware name> in the category <malware category> has been found on this site.
ERR_MALWARE_SPECIFIC_OUTGOING Security: Malware Detected	Block page that is displayed when malware is detected when uploading a file.	Based on your organization's policy, the upload of the file to URL (<URL>) has been blocked because the file was detected to contain malware that will be harmful to the receiving end's network security. Malware Name: <malware name> Malware Category: <malware category>
ERR_NATIVE_FTP_DENIED	Block message displayed in native FTP clients when the native FTP transaction is blocked.	530 Login denied

File Name and Notification Title	Notification Description	Notification Text
ERR_NO_MORE_FORWARDS No More Forwards	Error page that is displayed when the appliance has detected a forward loop between the Web Proxy and another proxy server on the network. The Web Proxy breaks the loop and displays this message to the client.	The request for the page <URL> failed. The server address <hostname> may be invalid, or you may need to specify a port number to access this server.
ERR_POLICY Policy: General	Block page that is displayed when the request is blocked by any policy setting.	Based on your organization's Access Policies, access to this web site <URL> has been blocked.
ERR_PROTOCOL Policy: Protocol	Block page that is displayed when the request is blocked based on the protocol used.	Based on your organization's Access Policies, this request has been blocked because the data transfer protocol "<protocol type>" is not allowed.
ERR_PROXY_AUTH_REQUIRED Proxy Authorization Required	Notification page that is displayed when users must enter their authentication credentials to continue. This is used for explicit transaction requests.	Authentication is required to access the Internet using this system. A valid user ID and password must be entered when prompted.
ERR_PROXY_PREVENT_MULTIPLE_LOGIN Already Logged In From Another Machine	Block page that is displayed when someone tries to access the web using the same username that is already authenticated with the Web Proxy on a different machine. This is used when the User Session Restrictions global authentication option is enabled.	Based on your organization's policies, the request to access the Internet was denied because this user ID has an active session from another IP address. If you want to login as a different user, click on the button below and enter a different a user name and password.
ERR_PROXY_REDIRECT Redirect	Redirection page.	This request is being redirected. If this page does not automatically redirect, click here to proceed.
ERR_PROXY_UNACKNOWLEDGED Policy Acknowledgment	End-user acknowledgment page. For more information, see On-Box End-User Notification Pages, page 16-4 .	Please acknowledge the following statements before accessing the Internet. Your web transactions will be automatically monitored and processed to detect dangerous content and to enforce organization's policies. By clicking the link below, you acknowledge this monitoring and accept that data about the sites you visit may be recorded. You will be periodically asked to acknowledge the presence of the monitoring system. You are responsible for following organization's policies on Internet access. Click here to accept this statement and access the Internet.

File Name and Notification Title	Notification Description	Notification Text
ERR_PROXY_UNLICENSED Proxy Not Licensed	Block page that is displayed when there is no valid license key for the Web Security appliance Web Proxy.	Internet access is not available without proper licensing of the security device. Please contact <contact name> <email address> and provide the code shown below. Note To access the management interface of the security device, enter the configured IP address with port.
ERR_RANGE_NOT_SATISFIABLE Range Not Satisfiable	Error page that is displayed when the requested range of bytes cannot be satisfied by the web server.	The system cannot process this request. A non-standard browser may have generated an invalid HTTP request. If you are using a standard browser, please retry the request.
ERR_REDIRECT_PERMANENT Redirect Permanent	Internal redirection page.	The page <URL> is being redirected to <redirected URL>.
ERR_REDIRECT_REPEAT_REQUEST Redirect	Internal redirection page.	Please repeat your request.
ERR_SAAS_AUTHENTICATION Policy: Access Denied	Notification page that is displayed when users must enter their authentication credentials to continue. This is used for accessing applications.	Based on your organization's policy, the request to access <URL> was redirected to a page where you must enter the login credentials. You will be allowed to access the application if authentication succeeds and you have the proper privileges.
ERR_SAAS_AUTHORIZATION Policy: Access Denied	Block page that is displayed when users try to access a application that they have no privilege to access.	Based on your organization's policy, the access to the application <URL> is blocked because you are not an authorized user. If you want to login as a different user, enter a different username and password for a user that is authorized to access this application.
ERR_SAML_PROCESSING Policy: Access Denied	Error page that is displayed when an internal process fails trying to process the single sign-on URL for accessing a application.	The request to access <user name> did not go through because errors were found during the process of the single sign on request.
ERR_SERVER_NAME_EXPANSION Server Name Expansion	Internal redirection page that automatically expands the URL and redirects users to the updated URL.	The server name <hostname> appears to be an abbreviation, and is being redirected to <redirected URL>.
ERR_URI_TOO_LONG URI Too Long	Block page that is displayed when the URL length is too long.	The requested URL was too long and could not be processed. This may represent an attack on your network. Please contact <contact name> <email address> and provide the code shown below.

File Name and Notification Title	Notification Description	Notification Text
ERR_WBRS Security: Malware Risk	Block page that is displayed when the Web Reputation Filters block the site due to a low web reputation score.	Based on your organization's access policies, this web site <URL> has been blocked because it has been determined by Web Reputation Filters to be a security threat to your computer or the organization's network. This web site has been associated with malware/spyware. Threat Type: %o Threat Reason: %O
ERR_WEBCAT Policy: URL Filtering	Block page that is displayed when users try to access a website in a blocked URL category.	Based on your organization's Access Policies, access to this web site <URL> has been blocked because the web category "<category type>" is not allowed.
ERR_WWW_AUTH_REQ UIRED WWW Authorization Required	Notification page that is displayed when the requested server requires users to enter their credentials to continue.	Authentication is required to access the requested web site <hostname>. A valid user ID and password must be entered when prompted.



Generate Reports to Monitor End-user Activity

- [Overview of Reporting, page 17-1](#)
- [Using the Reporting Tab, page 17-2](#)
- [Enabling Centralized Reporting, page 17-8](#)
- [Scheduling Reports, page 17-8](#)
- [Generating Reports On Demand, page 17-10](#)
- [Archived Reports, page 17-10](#)
- [SNMP Monitoring, page 17-11](#)

Overview of Reporting

The Web Security appliance generates high-level reports, allowing you to understand what is happening on the network and also allows you to view traffic details for a particular domain, user, or category. You can run reports to view an interactive display of system activity over a specific period of time, or you can schedule reports and run them at regular intervals.

Related Topics

- [Printing and Exporting Reports from Report Pages, page 17-7](#)

Working with Usernames in Reports

When you enable authentication, reports list users by their usernames when they authenticate with the Web Proxy. By default, usernames are written as they appear in the authentication server. However, you can choose to make usernames unrecognizable in all reports.



Note

Administrators always see usernames in reports.

Step 1 Choose **Security Services > Reporting**, and click **Edit Settings**.

Step 2 Under Local Reporting, select **Anonymize usernames in reports**.

Step 3 **Submit** and **Commit Changes**.

Report Pages

The Web Security appliance offers the following reports:

- Overview
- Users
- Web Sites
- URL Categories
- Application Visibility
- Anti-Malware
- Client Malware Risk
- Web Reputation Filters
- Layer-4 Traffic Monitor
- Reports by User Location
- Web Tracking
- System Capacity
- System Status

Using the Reporting Tab

The Reporting tab provides several options for viewing system data. The report pages provide an overview of system activity and support multiple options for viewing system data. You can also search each page for website and client-specific data.

You can perform the following tasks on most reports on the Reporting tab:

Option	Link to Task
Change the time range displayed in a report	Changing the Time Range, page 17-2
Search for specific clients and domains	Searching Data, page 17-3
Choose which data to display in charts	Choosing Which Data to Chart, page 17-4
Choose and sort columns	Related Topics, page 17-4
Export reports to external files	Printing and Exporting Reports from Report Pages, page 17-7

Changing the Time Range

You can update the data displayed for each security component using the Time Range field. This option allows you to generate updates for predefined time ranges and it allows you to define custom time ranges from a specific start time to a specific end time.

**Note**

The time range you select is used throughout all of the report pages until you select a different value in the Time Range menu.

Time Range	Data is returned in...
Hour	Sixty (60) complete minutes plus up to 5 additional minutes.
Day	One hour intervals for the last 24 hours and including the current partial hour.
Week	One day intervals for the last 7 days plus the current partial day.
Month (30 days)	One day intervals for the last 30 days plus the current partial day.
Yesterday	The last 24 hours (00:00 to 23:59) using the Web Security appliance defined time zone.
Custom Range	The custom time range defined by the user. When you choose Custom Range, a dialog box appears where you can enter the start and end times.

**Note**

All reports display date and time information based on the systems configured time zone, shown as a Greenwich Mean Time (GMT) offset. However, data exports display the time in GMT to accommodate multiple systems in multiple time zones around the world.

Searching Data

Some reports include a field that allow you to search for particular data points. When you search for data, the report refines the report data for the particular data set you are searching. You can search for values that exactly match of the string you enter, or for values that start with the string you enter. The following report pages include search fields:

Search Fields	Description
Users	Search for a user by user name or client IP address
Web Sites	Search for a server by domain or server IP address
URL Categories	Search for a URL category
Application Visibility	Search for an application name that the AVC engine monitors and blocks
Client Malware Risk	Search for a user by user name or client IP address

**Note**

You need to configure authentication to view client user IDs as well as client IP addresses.

Choosing Which Data to Chart

The default charts on each Web Reporting page display commonly-referenced data, but you can choose to chart different data instead. If a page has multiple charts, you can change each chart. The chart options are the same as the columns headings of the table(s) in the report.

-
- Step 1** Click the **Chart Options** link below a chart.
- Step 2** Choose the data to display.
- Step 3** Click **Done**.
-

Related Topics

- [Related Topics, page 17-4](#)

Custom Reports

You can create a custom report page by assembling charts (graphs) and tables from existing report pages.

To	Do This
Add modules to your custom report page	See: <ul style="list-style-type: none"> • Creating Your Custom Report Page, page 17-5. • Creating Your Custom Report Page, page 17-5
View your custom report page	<ol style="list-style-type: none"> 1. Choose Reporting > My Reports. 2. Select the time range to view. The time range selected applies to all reports, including all modules on the My Reports page. <p>Newly-added modules appear at the top of the relevant section.</p>
Rearrange modules on your custom report page	Drag and drop modules into the desired location.
Delete modules from your custom report page	Click the [X] in the top right corner of the module.
Generate a PDF or CSV version of your custom report	See: <ul style="list-style-type: none"> • Generating Reports On Demand, page 17-10
Periodically generate a PDF or CSV version of your custom report	See: <ul style="list-style-type: none"> • Scheduling Reports, page 17-8

Creating Your Custom Report Page

Before You Begin

- Be aware that search results, including Web Tracking search results cannot be added to custom reports.
- Delete any default modules that you do not need by clicking the [X] in the top right corner of the module.

Step 1 Use one of the following methods to add a module to your custom report page:



Note Some modules are available only using one of these methods. If you cannot add a module using one method, try another method.

- Navigate to the report page that has the module that you want to add, then click the [+] button at the top of the module.
- Go to **Reporting > My Reports**, click the [+] button at the top of one of the sections, then select the report module that you want to add. You may need to click the [+] button in each section on the My Reports page in order to find the module that you are looking for.

You can add each module only once; if you have already added a particular module to your report, the option to add it will not be available.

Step 2 If you add a module that you have customized (for example, by adding, deleting, or reordering columns, or by displaying non-default data in the chart), customize the modules on the My Reports page.

Modules are added with default settings. Time range of the original module is not maintained.

Step 3 If you add a chart that includes a separate legend (for example, a graph from the Overview page), add the legend separately. If necessary, drag and drop it into position beside the data it describes.

Working with Columns on Report Pages

Each page has interactive column headings that can be configured to sort the data in each column specific to your needs for viewing data on that page.



Note Not every column is available for every report page. Click the Columns link for each report page to view the available columns.

Column Name	Description
Domain or Realm	The domain or realm of the user displayed in text format.
User ID or Client IP	The username or client IP address of the user displayed in text format.
Bandwidth Used	The amount of bandwidth that is used by a particular user or action. Bandwidth units are displayed in Bytes or percentage.

Column Name	Description
Bandwidth Saved by Blocking	The amount of bandwidth that has been saved due to blocking certain transactions. Bandwidth units are displayed in Bytes
Time Spent	<p>Amount of time spent on a web page. For purposes of investigating a user, the time spent by the user on each URL category. When tracking a URL, the time spent by each user on that specific URL.</p> <p>To calculate the time spent, AsyncOS assigns each active user with 60 seconds of time for activity during a minute. At the end of the minute, the time spent by each user is evenly distributed among the different domains the user visited. For the purposes of the time spent value, considering the following notes:</p> <p>Note Units displayed in Hours:Minutes format.</p>
Allowed URL Category	The number and type of categories that have been allowed.
Monitored URL Category	The number and type of categories that are being monitored.
Warned URL Category	The number and type of categories that have initiated a warning.
Blocked by URL Category	The transaction that has been blocked due to URL Category.
Blocked by Application or Application Type	The application that has been blocked due to application type.
Blocked by Web Reputation	The transaction that has been blocked due to web reputation.
Blocked by Anti-Malware	The transactions blocked by Anti-Malware.
Other Blocked Transactions	All other transactions that have been blocked.
Transactions with Bandwidth Limit	The number of transactions that have a bandwidth limit.
Transactions without Bandwidth Limit	The number of transactions that do not have a bandwidth limit.
Transactions Blocked by Application	The number of transactions blocked by a specific application type.
Warned Transactions	All transactions that rendered a warning to the user.
Transactions Completed	The transactions completed by a user.
Transactions Blocked	All transactions that have been blocked.
Total Transactions	The total number of transactions that have occurred.



Note Units displayed in transaction type.

Configuring Columns on Report Pages

- Step 1** Choose **Reporting > Report_Name**.
- Step 2** Click the **Columns** link that appears in the lower right corner of a report.

- Step 3** Select each column to display by clicking the checkbox next to each column in the pop-up window and click **Done**.

Subdomains vs. Second-Level Domains in Reporting and Tracking

In reporting and tracking searches, second-level domains (regional domains listed at <http://george.surbl.org/two-level-tlds>) are treated differently from subdomains, even though the two domain types may appear to be the same. For example:

- Reports will not include results for a two-level domain such as `co.uk`, but will include results for `foo.co.uk`. Reports include subdomains under the main corporate domain, such as `cisco.com`.
- Tracking search results for the regional domain `co.uk` will not include domains such as `foo.co.uk`, while search results for `cisco.com` will include subdomains such as `subdomain.cisco.com`.

Printing and Exporting Reports from Report Pages

You can generate a printer-friendly formatted PDF version of any of the report pages by clicking the **Printable (PDF)** link at the top-right corner of the page. You can also export raw data as a comma-separated value (CSV) file by clicking the **Export** link.

Because CSV exports include only raw data, exported data from a web-based report page may not include calculated data such as percentages, even if that data appears in the web-based report.

Exporting Report Data

Most reports include an **Export** link that allows you to export raw data to a comma-separated values (CSV) file. After exporting the data to a CSV file, you can access and manipulate the data in it using applications such as Microsoft Excel.

The exported CSV data displays all message tracking and reporting data in Greenwich Mean Time (GMT) regardless of what is set on the Web Security appliance. The purpose of the GMT time conversion is to allow data to be used independently from the appliance or when referencing data from appliances in multiple time zones.

The following example is an entry from a raw data export of the Anti-Malware category report, where Pacific Daylight Time (PDT) is displayed as GMT - 7 hours:

```
Begin Timestamp, End Timestamp, Begin Date, End Date, Name, Transactions Monitored,
Transactions Blocked, Transactions Detected
1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525,
2100, 2625
```

Category Header	Value	Description
Begin Timestamp	1159772400.0	Query start time in number of seconds from epoch.
End Timestamp	1159858799.0	Query end time in number of seconds from epoch.
Begin Date	2006-10-02 07:00 GMT	Date the query began.
End Date	2006-10-03 06:59 GMT	Date the query ended.

(continued)

Category Header	Value	Description
Name	Adware	Name of the malware category.
Transactions Monitored	525	Number of transactions monitored.
Transactions Blocked	2100	Number of transactions blocked.
Transactions Detected	2625	Total number of transactions: Number of transactions detected + Number of transactions blocked.

**Note**

Category headers are different for each type of report.

**Note**

If you export localized CSV data, the headings may not be rendered properly in some browsers. This occurs because some browsers may not use the proper character set for the localized text. To work around this problem, you can save the file to your local machine, and open the file in any web browser using **File > Open**. When you open the file, select the character set to display the localized text.

Enabling Centralized Reporting

When the Web Security appliance is managed by a Security Management appliance, you can choose which appliance displays reports on the web traffic that is processed by the Web Security appliance. You might want to enable Centralized Reporting when the Security Management appliance manages multiple Web Security appliances.

**Note**

When you enable Centralized Reporting, only the System Capacity and System Status reports are available on the Web Security appliance. To view the other reports, connect to the Security Management appliance.

Step 1 Choose **Security Services > Reporting** and click **Edit Settings**.

Step 2 Choose **Centralized Reporting**.

Step 3 **Submit** and **Commit Changes**.

Scheduling Reports

You can schedule reports to run on a daily, weekly, or monthly basis. Scheduled reports can be configured to include data for the previous day, previous seven days, or previous month.

You can schedule reports for the following types of reports:

- Overview

- Users
- Web Sites
- URL Categories
- Application Visibility
- Anti-Malware
- Client Malware Risk
- Web Reputation Filters
- Layer-4 Traffic Monitor
- Reports by User Location
- System Capacity

Adding a Scheduled Report

-
- Step 1** Choose **Reporting > Scheduled Reports** and click **Add Scheduled Report**.
- Step 2** Select a report type.
- Step 3** Enter a title for the report. To avoid creating multiple reports with the same name, consider using a descriptive title.
- Step 4** Select a time range for the data included in the report.
- Step 5** Choose the format for the generated report.
The default format is PDF. Most reports also allow you to save raw data as a CSV file.
- Step 6** Depending on the type of report you configure, you can specify different report options, such as the number of rows to include and by which column to sort the data. Configure these options as necessary.
- Step 7** In the Schedule section, choose whether to run the report daily, weekly, or monthly and at what time.
- Step 8** In the Email field, enter the email address to where to send the generated report.
If you do not specify an email address, the report is archived only.
- Step 9** **Submit** and **Commit Changes**.
-

Editing Scheduled Reports

-
- Step 1** Choose **Reporting > Scheduled Reports**.
- Step 2** Select the report title from the list.
- Step 3** Modify settings.
- Step 4** **Submit** and **Commit Changes**.
-

Deleting Scheduled Reports

-
- Step 1** Choose **Reporting > Scheduled Reports**.
 - Step 2** Select the check boxes corresponding to the reports that you want to delete.
 - Step 3** To remove all scheduled reports, select the All check box.
 - Step 4** **Delete** and **Commit Changes**.



Note Archived versions of deleted reports are not deleted.

Generating Reports On Demand

-
- Step 1** Choose **Reporting > Archived Reports**.
 - Step 2** Click **Generate Report Now**.
 - Step 3** Select a report type and edit the title.
 - Step 4** Select a time range for the data included in the report.
 - Step 5** Choose the format for the generated report.
The default format is PDF. Most reports also allow you to save raw data as a CSV file.
 - Step 6** Depending on the type of report you configure, you can specify different report options, such as the number of rows to include and by which column to sort the data. Configure these options as necessary.
 - Step 7** Select whether to archive the report (if so, the report will appear on the Archived Reports page).
 - Step 8** Specify whether to email the report, and list the email addresses of the recipients.
 - Step 9** Click **Deliver this Report** to generate the report.
 - Step 10** **Commit Changes**.
-

Archived Reports

The **Reporting > Archived Reports** page lists available archived reports. Report names in the Report Title column are interactive and link to a view of each report. The Show menu filters the types of reports that are listed. Interactive column headings can be used to sort the data in each column.

The appliance stores up to 12 instances of each scheduled report (up to 1000 reports). Archived reports are stored in the `/periodic_reports` directory on the appliance. Archived reports are deleted automatically. As new reports are added, older reports are removed to keep the number at 1000. The limit of 12 instances applies to each scheduled report with the same name and time range.

SNMP Monitoring

The AsyncOS operating system supports system status monitoring via SNMP (Simple Network Management Protocol). This includes Cisco's Enterprise MIB, `asyncosecwebsecurityappliance-mib.txt`. The `asyncosecwebsecurityappliance-mib` helps administrators better monitor system health. In addition, this release implements a read-only subset of MIB-II as defined in RFCs 1213 and 1907. (For more information about SNMP, see RFCs 1065, 1066, and 1067.) Please note:

- SNMP requests are serviced on the P1 interface.
- SNMP is **off** by default.
- SNMP SET operations (configuration) are not implemented.
- AsyncOS supports SNMPv1, v2, and v3.
- The use of SNMPv3 with password authentication and DES Encryption is mandatory to enable this service. (For more information on SNMPv3, see RFCs 2571-2575.) You are required to set a SNMPv3 passphrase of at least 8 characters to enable SNMP system status monitoring. The first time you enter a SNMPv3 passphrase, you must re-enter it to confirm. The `snmpconfig` command “remembers” this phrase the next time you run the command.
- The SNMPv3 username is: `v3get`.

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 serv.example.com
```

- If you use only SNMPv1 or SNMPv2, you must set a community string. The community string does not default to `public`.
- For SNMPv1 and SNMPv2, you must specify a network from which SNMP GET requests are accepted.
- To use traps, an SNMP manager (not included in AsyncOS) must be running and its IP address entered as the trap target. (You can use a hostname, but if you do, traps will only work if DNS is working.)

Use the `snmpconfig` command to configure SNMP system status for the appliance. After you choose and configure values for an interface, the appliance responds to SNMPv3 GET requests. These version 3 requests must include a matching password. By default, version 1 and 2 requests are rejected. If enabled, version 1 and 2 requests must have a matching community string.

MIB Files

Cisco provides “enterprise” MIBs for Email and Web Security appliances as well as a “Structure of Management Information” (SMI) file:

- `asyncosecwebsecurityappliance-mib.txt` — an SNMPv2 compatible description of the Enterprise MIB for Web Security appliances.
- `ASYNCOSEC-MAIL-MIB.txt` — an SNMPv2 compatible description of the Enterprise MIB for Email Security appliances.
- `IRONPORT-SMI.txt` — defines the role of the `asyncosecwebsecurityappliance-mib`.

These files are available on the documentation CD included with your Cisco Web Security Appliance appliance. You can also find these files here:

```
http://www.cisco.com/en/US/customer/products/ps10164/tsd\_products\_support\_series\_home.html
```

Hardware Objects

Hardware sensors conforming to the Intelligent Platform Management Interface Specification (IPMI) report temperature, fan speed, and power supply status.

The number displayed is the number of instances of that object that can be monitored. For example, you can query the RPMs for 4 fans in the S350 appliance.

Model	Ambient Temp	Fans	Power Supply	Disk Status	NIC Link
S160	1	2	1	2	6
S350	1	4	2	6	6
S360	1	4	2	4	6
S650	1	4	2	6	6
S660	1	4	2	6	6

Hardware Traps

Model	High Temp (Ambient)	Fan Failure	Power Supply	RAID	Link
S160/S350/S360/S650/S660	47C	0 RPMs	Status Change	Status Change	Status Change

Status change traps are sent when the status changes. Fan Failure and high temperature traps are sent every 5 seconds. The other traps are failure condition alarm traps - they are sent once when the state changes (healthy to failure). Temperatures within 10 per cent of the critical value may be a cause for concern.



Note

Failure condition alarm traps represent a critical failure of the individual component, but may not cause a total system failure.

SNMP Traps

SNMP provides the ability to send traps, or notifications, to advise an administration application when one or more conditions have been met. Traps are network packets that contain data relating to a component of the system sending the trap. Traps are generated when a condition has been met on the SNMP agent (in this case, the Cisco Web Security Appliance appliance). After the condition has been met, the SNMP agent then forms an SNMP packet and sends it over port 162, the standard SNMP trap port. In the example below, the trap target of 10.1.1.29 and the Trap Community string are entered. This is the host running the SNMP management console software that will receive the SNMP traps from the appliance.

You can configure SNMP traps (enable or disable specific traps) when you enable SNMP for an interface. To specify multiple trap targets: when prompted for the trap target, you may enter up to 10 comma separated IP addresses.

CLI Example

In this example, the `snmpconfig` command is used to enable SNMP on the “PublicNet” interface on port 161. A passphrase for version 3 is entered and then re-entered for confirmation. The system is configured to service version 1 and 2 requests, and the community string `public` is entered for GET requests from those versions 1 and 2. The trap target of `10.1.1.29` is entered. Finally, system location and contact information is entered.

```
example.com> snmpconfig

Current SNMP settings:

SNMP Disabled.

Choose the operation you want to perform:

- SETUP - Configure SNMP.

[ ]> setup

Do you want to enable SNMP? [N]> y

Please choose an IP interface for SNMP requests.

1. Management (192.168.1.1/24: wsa01-vmw1-tpub.qa)

[1]>

Enter the SNMPv3 passphrase.

>

Please enter the SNMPv3 passphrase again to confirm.

>

Which port shall the SNMP daemon listen on?

[161]>

Service SNMP V1/V2c requests? [N]> y
```

Enter the SNMP V1/V2c community string.

```
[> public
```

From which network shall SNMP V1/V2c requests be allowed?

```
[192.168.1.1]>
```

Enter the Trap target as a host name, IP address or list of IP addresses separated by commas (IP address preferred). Enter "None" to disable traps.

```
[None]> 10.1.1.29
```

Enter the Trap Community string.

```
[> tcomm
```

Enterprise Trap Status

1. CPUUtilizationExceeded	Disabled
2. RAIDStatusChange	Enabled
3. connectivityFailure	Disabled
4. fanFailure	Enabled
5. highTemperature	Enabled
6. keyExpiration	Enabled
7. linkDown	Enabled
8. linkUp	Enabled
9. memoryUtilizationExceeded	Disabled
10. powerSupplyStatusChange	Enabled
11. resourceConservationMode	Enabled
12. updateFailure	Enabled
13. upstream_proxy_failure	Enabled

Do you want to change any of these settings? [N]> **y**

Do you want to disable any of these traps? [Y]> **n**

Do you want to enable any of these traps? [Y]> **y**

Enter number or numbers of traps to enable. Separate multiple numbers with commas.

[]> **1,3**

What threshold would you like to set for CPU utilization?

[95]>

What URL would you like to check for connectivity failure?

[http://downloads.ironport.com]>

Enterprise Trap Status

1. CPUUtilizationExceeded	Enabled
2. RAIDStatusChange	Enabled
3. connectivityFailure	Enabled
4. fanFailure	Enabled
5. highTemperature	Enabled
6. keyExpiration	Enabled
7. linkDown	Enabled
8. linkUp	Enabled
9. memoryUtilizationExceeded	Disabled
10. powerSupplyStatusChange	Enabled
11. resourceConservationMode	Enabled
12. updateFailure	Enabled
13. upstream_proxy_failure	Enabled

```
Do you want to change any of these settings? [N]>
```

```
Enter the System Location string.
```

```
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3
```

```
Enter the System Contact string.
```

```
[snmp@localhost]> Joe Administrator, x8888
```

```
Current SNMP settings:
```

```
Listening on interface "Management" 192.168.1.1 port 161.
```

```
SNMP v3: Enabled.
```

```
SNMP v1/v2: Enabled, accepting requests from subnet 192.168.1.1.
```

```
SNMP v1/v2 Community String: public
```

```
Trap target: 10.1.1.29
```

```
Location: Network Operations Center - west; rack #30, position 3
```

```
System Contact: Joe Administrator, x8888
```

```
Choose the operation you want to perform:
```

```
- SETUP - Configure SNMP.
```

```
[ ]>
```

```
example.com>
```




Web Security Appliance Reports

- [Overview Page](#), page 23-1
- [Users Page](#), page 18-2
- [Web Sites Page](#), page 18-3
- [URL Categories Page](#), page 18-3
- [Application Visibility Page](#), page 18-4
- [Anti-Malware Page](#), page 18-5
- [Advanced Malware Protection Page](#), page 18-5
- [File Analysis Page](#), page 18-6
- [AMP Verdict Updates Page](#), page 18-6
- [Client Malware Risk Page](#), page 18-6
- [Web Reputation Filters Page](#), page 18-8
- [L4 Traffic Monitor Page](#), page 18-8
- [SOCKS Proxy Page](#), page 18-9
- [Reports by User Location Page](#), page 18-9
- [Web Tracking Page](#), page 18-10
- [System Capacity Page](#), page 18-14
- [System Status Page](#), page 18-15

Overview Page

The **Reporting > Overview** page provides a synopsis of the activity on the Web Security appliance. It includes graphs and summary tables for web traffic processed by the Web Security appliance.

Section	Description
Time Range (drop-down list)	A menu that allows you to choose the time range of the data contained in the report.
Total Web Proxy Activity	Displays the actual number of transactions (vertical scale) as well as the approximate date that the (web Proxy) activity occurred (horizontal timeline).

(continued)

Section	Description
Web Proxy Summary	Allows you to view the percentage of Web Proxy activity that are suspect or clean Web Proxy activity.
L4 Traffic Monitor Summary	Reports on traffic monitored and blocked by the L4 Traffic Monitor.
Suspect Transactions	Allows you to view the web transactions that have been labeled as suspect by the various security components. Displays the actual number of transactions as well as the approximate date that the activity occurred.
Suspect Transactions Summary	Allows you to view the percentage of blocked or warned transactions that are suspect.
Top URL Categories by Total Transactions	Displays the top 10 URL categories that have been blocked.
Top Application Types by Total Transactions	Displays the top application types that have been blocked by the AVC engine.
Top Malware Categories Detected	Displays all malware categories that have been detected.
Top Users Blocked or Warned Transactions	Displays the users that are generating the blocked or warned transactions. Authenticated users are displayed username and unauthenticated users are displayed by IP address.

Users Page

The **Reporting > Users** page provides several links that allows you to view web traffic information for individual users. You can view how much time users on the network have spent on the Internet or on a particular website or URL, and how much bandwidth users have used.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Top Users by Transactions Blocked	Lists the users (vertical scale) that have the greatest number of blocked transactions (horizontal scale).
Top Users by Bandwidth Used	Displays the users (vertical scale) that are using the most bandwidth on the system (horizontal scale represented in gigabyte usage).
Users Table	Lists individual users and displays multiple statistics on each user.

User Details Page

The **User Details** page displays information about a specific user selected in the Users Table on the **Reporting > Users** page.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
URL Categories by Total Transactions	Lists the specific URL categories that a specific user is using.
Trend by Total Transaction	Displays at what times the user accessed the web.
URL Categories Matched	Shows all matched URL categories during a specified time range for both completed and blocked transactions.
Domains Matched	Displays information about a specific Domain or IP address that this user has accessed.
Applications Matched	Displays specific application that a specific user is using as detected by the AVC engine.
Malware Threats Detected	Displays the top malware threats that a specific user is triggering.
Policies Matched	Displays a specific policy that is being enforced on this particular user.

Web Sites Page

The **Reporting > Web Sites** page is an overall aggregation of the activity that is happening on the Web Security appliance.

Section	Description
Time Range (drop-down list)	Menu allows you to choose the time range of the data contained in the report.
Top Domains by Total Transactions	Lists the top domains that are being visited on the site in a graph format.
Top Domains by Transactions Blocked	Lists the top domains that triggered a block action to occur per transaction in a graph format.
Domains Matched	Lists the domains that are that are being visited on the site in an interactive table.

URL Categories Page

The **Reporting > URL Categories** page can be used to view the URL categories that are being visited by users on the network. The URL Categories page can be used in conjunction with the [Application Visibility Page](#) and the [Users Page](#) to investigate a particular user and also what types of applications or websites that a particular user is trying to access.

**Note**

The set of predefined URL categories is occasionally updated.

Section	Description
Time Range (drop-down list)	Choose the time range for your report.
Top URL Categories by Total Transactions	This section lists the top URL categories that are being visited on the site in a graph format.
Top URL Categories by Blocked and Warned Transactions	Lists the top URL that triggered a block or warning action to occur per transaction in a graph format.
URL Categories Matched	Shows the disposition of transactions by URL category during the specified time range, plus bandwidth used and time spent in each category. If the percentage of uncategorized URLs is higher than 15-20%, consider the following options: <ul style="list-style-type: none"> • For specific localized URLs, you can create custom URL categories and apply them to specific users or group policies. • You can report uncategorized and misclassified URLs to the Cisco for evaluation and database update. • Verify that Web Reputation Filtering and Anti-Malware Filtering are enabled.

URL Category Set Updates and Reports

The set of predefined URL categories may periodically be updated automatically on your Web Security appliance.

When these updates occur, old category names will continue to appear in reports until the data associated with the older categories is too old to be included in reports. Report data generated after a URL category set update will use the new categories, so you may see both old and new categories in the same report.

Application Visibility Page

The **Reporting > Application Visibility** page shows the applications and application types used and blocked as detected by the Application Visibility and Control engine.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Top Application Types by Total Transactions	This section lists the top application types that are being visited on the site in a graph format.
Top Applications by Blocked Transactions	Lists the top application types that triggered a block action to occur per transaction in a graph format.

(continued)

Section	Description
Application Types Matched	Allows you to view granular details about the application types listed in the Top Applications Type by Total Transactions graph.
Applications Matched	Shows all the application during a specified time range.

Anti-Malware Page

The **Reporting > Anti-Malware** page allows you to monitor and identify malware detected by the Cisco IronPort DVS engine.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Top Malware Categories Detected	Displays the top malware categories detected by the DVS engine.
Top Malware Threats Detected	Displays the top malware threats detected by the DVS engine.
Malware Categories	Displays information about particular malware categories that are shown in the Top Malware Categories Detected section.
Malware Threats	Displays information about particular malware threats that are shown in the Top Malware Threats section.

Malware Category Report Page

-
- Step 1** Choose **Reporting > Anti-Malware**.
 - Step 2** In the Malware Categories interactive table, click on a category in the Malware Category column.
-

Malware Threat Report Page

-
- Step 1** Choose **Reporting > Anti-Malware**.
 - Step 2** In the Malware Threat table, click on a category in the Malware Category column.
-

Advanced Malware Protection Page

See [File Reputation and File Analysis Reporting and Tracking](#), page 16-13.

File Analysis Page

See [File Reputation and File Analysis Reporting and Tracking](#), page 16-13.

AMP Verdict Updates Page

See [File Reputation and File Analysis Reporting and Tracking](#), page 16-13.

Client Malware Risk Page

The **Reporting > Client Malware Risk** page is a security-related reporting page that can be used to monitor client malware risk activity. The Client Malware Risk page also lists client IP addresses involved in frequent malware connections, as identified by the L4 Traffic Monitor (L4TM).

Section	Description
Time Range (drop-down list)	A menu that allows you to choose the time range of the data contained in the report.
Web Proxy: Top Clients by Malware Risk	This chart displays the top ten users that have encountered a malware risk.
L4 Traffic Monitor: Malware Connections Detected	This chart displays the IP addresses of the computers in your organization that most frequently connect to malware sites.
Web Proxy: Clients by Malware Risk	The Web Proxy: Clients by Malware Risk table shows detailed information about particular clients that are displayed in the Web Proxy: Top Clients by Malware Risk section.
L4 Traffic Monitor: Clients by Malware Risk	This table displays IP addresses of computers in your organization that frequently connect to malware sites.

Client Detail Page for Web Proxy - Clients by Malware Risk

The Client Details page shows all the web activity and malware risk data for a particular client during the specified time range.

-
- Step 1** Choose **Reporting > Client Malware Risk**.
- Step 2** In the **Web Proxy - Client Malware Risk** section, click on a user in the “User ID / Client IP Address” column.
-

Related Topics

- [User Details Page, page 23-3](#)

Web Reputation Filters Page

The **Reporting > Web Reputation Filters** page is a security-related reporting page that allows you to view the results of your set Web Reputation Filters for transactions during a specified time range.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Web Reputation Actions (Trend)	Displays the total number of web reputation actions (vertical) against the time specified (horizontal timeline).
Web Reputation Actions (Volume)	Displays the web reputation action volume in percentages by transactions.
Web Reputation Threat Types by Blocked Transactions	Displays the threat types that were blocked due to a low reputation score.
Web Reputation Threat Types by Scanned Further Transactions	Displays the threat types that resulted in a reputation score that indicated to scan the transaction.
Web Reputation Actions (Breakdown by Score)	Displays the web reputation scores broken down for each action.

L4 Traffic Monitor Page

The **Reporting > L4 Traffic Monitor** page is a security-related reporting page that displays information about malware ports and malware sites that the L4 Traffic Monitor has detected during the specified time range. It also displays IP addresses of clients that frequently encounter malware sites.

The L4 Traffic Monitor listens to network traffic that comes in over all ports on the appliance and matches domain names and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic.

Section	Description
Time Range (drop-down list)	A menu that allows you to choose a time range on which to report.
Top Client IPs	Displays, in graph format, the IP addresses of computers in your organization that most frequently connect to malware sites.
Top Malware Sites	Displays, in graph format, the top malware domains detected by the L4 Traffic Monitor.
Client Source IPs	Displays the IP addresses of computers in your organization that frequently connect to malware sites.
Malware Ports	Displays the ports on which the L4 Traffic Monitor has most frequently detected malware.
Malware Sites Detected	Displays the domains on which the L4 Traffic Monitor most frequently detects malware.

SOCKS Proxy Page

The **Reporting > SOCKS Proxy** Page allows you to view data and trends for transactions processed through the SOCKS proxy, including information about top destinations and users.

Reports by User Location Page

The **Reporting > Reports by User Location** page allows you to find out what activities your local and remote users are conducting.

Activities include:

- URL categories that are being accessed by the local and remote users.
- Anti-Malware activity that is being triggered by sites the local and remote users are accessing.
- Web Reputation of the sites being accessed by the local and remote users.
- Applications that are being accessed by the local and remote users.
- Users (local and remote).
- Domains accessed by local and remote users.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Total Web Proxy Activity: Remote Users	Displays the activity of your remote users (vertical) over the specified time (horizontal).
Web Proxy Summary	Displays a summary of the activities of the local and remote users on the network.
Total Web Proxy Activity: Local Users	Displays the activity of your remote users (vertical) over the specified time (horizontal).
Suspect Transactions Detected: Remote Users	Displays the suspect transactions that have been detected due to Access Policies defined for remote users (vertical) over the specified time (horizontal).
Suspect Transactions Summary	Displays a summary of suspected transactions of the remote users on the network.
Suspect Transactions Detected: Local Users	Displays the suspect transactions that have been detected due to Access Policies defined for your remote users (vertical) over the specified time (horizontal).
Suspect Transactions Summary	Displays a summary of suspected transactions of the local users on the network.

Web Tracking Page

Use the Web Tracking page to search for and get details about individual transactions or patterns of transactions that may be of concern. Depending on your needs, search in one or both of the following tabs:

Web Tracking Page	Link to Task
Transactions processed by the Web Proxy	Searching for Transactions Processed by the Web Proxy, page 18-10
Transactions processed by the L4 Traffic Monitor	Searching for Transactions Processed by the L4 Traffic Monitor, page 18-13
Transactions processed by the SOCKS Proxy	Searching for Transactions Processed by the SOCKS Proxy, page 18-13

Searching for Transactions Processed by the Web Proxy

You can use the **Proxy Services** tab on the **Reporting > Web Tracking** page to track and report on web usage for a particular user or for all users.

You can view search results for the type of transactions logged (blocked, monitored, warned, and completed) during a particular time period. You can also filter the data results using several criteria, such as URL category, malware threat, and application.



Note

The Web Proxy only reports on transactions that include an ACL decision tag other than "OTHER-NONE."

- Step 1** Choose **Reporting > Web Tracking**.
- Step 2** Click the **Proxy Services** tab.
- Step 3** Configure the settings.

Setting	Description
Time Range	Choose the time range on which to report.
User/Client IP	(Optional) Enter an authentication username as it appears in reports or a client IP address that you want to track. You can also enter an IP range in CIDR format. When you leave this field empty, the search returns results for all users.
Website	(Optional) Enter a website that you want to track. When you leave this field empty, the search returns results for all websites.
Transaction Type	Choose the type of transactions that you want to track, either All Transactions, Completed, Blocked, Monitored, or Warned.

- Step 4** (Optional) Expand the Advanced section and configure the fields to filter the web tracking results with more advanced criteria.

Setting	Description
URL Category	To filter by a URL category, select Filter by URL Category and type the first letter of a URL category by which to filter. Choose the category from the list that appears.
Application	To filter by an application, select Filter by Application and choose an application by which to filter. To filter by an application type, select Filter by Application Type and choose an application type by which to filter.
Policy	To filter by a policy group, select Filter by Policy and enter a policy group name by which to filter.
Advanced Malware Protection	See About Web Message Tracking and Advanced Malware Protection Features, page 16-16 .
Malware Threat	To filter by a particular malware threat, select Filter by Malware Threat and enter a malware threat name by which to filter. To filter by a malware category, select Filter by Malware Category and choose a malware category by which to filter.
WBRS	In the WBRS section, you can filter by web reputation score and by a particular web reputation threat. <ul style="list-style-type: none"> To filter by web reputation score, select Score Range and select the upper and lower values by which to filter. Or, you can filter for websites that have no score by selecting No Score. To filter by web reputation threat, select Filter by Reputation Threat and enter a web reputation threat by which to filter.
AnyConnect Secure Mobility	To filter by the location of users (either remote or local), select Filter by User Location and choose a user type by which to filter.
User Request	To filter by transactions that were initiated by the client, select Filter by User-Requested Transactions . Note When you enable this filter, the search results include some “best guess” transactions.

- Step 5** Click **Search**.

Results are sorted by time stamp, with the most recent result at the top.

The number in parentheses below the “Display Details” link is the number of related transactions spawned by the user-initiated transaction, such as images loaded, javascripts run, and secondary sites accessed.

- Step 6** (Optional) Click **Display Details** in the Transactions column to view more detailed information about each transaction.



Note If you need to view more than 1000 results, click the **Printable Download** link to obtain a CSV file that includes the complete set of raw data, excluding details of related transactions.



Tip If a URL in the results is truncated, you can find the full URL in the access log.

To view details for up to 500 related transactions, click the **Related Transactions** link.

Related Topics

- [URL Category Set Updates and Reports, page 18-4](#)
- [Malware Category Descriptions, page 13-17](#)
- [About Web Message Tracking and Advanced Malware Protection Features, page 16-16](#)

Searching for Transactions Processed by the L4 Traffic Monitor

The L4 Traffic Monitor tab on the **Reporting > Web Tracking** page provides details about connections to malware sites and ports. You can search for connections to malware sites by the following types of information:

- Time range
- Site, using IP address or domain
- Port
- IP address associated with a computer in your organization
- Connection type

The first 1000 matching search results are displayed.

Searching for Transactions Processed by the SOCKS Proxy

You can search for transactions that meet a variety of criteria, including blocked or completed transactions; users; and destination domain, IP address, or port.

-
- Step 1** Choose **Web > Reporting > Web Tracking**.
 - Step 2** Click the **SOCKS Proxy** tab.
 - Step 3** To filter results, click **Advanced**.
 - Step 4** Enter search criteria.
 - Step 5** Click **Search**.
-

Related Topics

- [SOCKS Proxy Page, page 18-9](#)

System Capacity Page

The **Reporting > System Capacity** page displays current and historical information about resource usage on the Web Security appliance.

When choosing time ranges for viewing data on the System Capacity page, the following is important to remember:

- **Hour Report.** The Hour report queries the minute table and displays the exact number of items, such as bytes and connection, that have been recorded by the appliance on an minute by minute basis over a 60 minute period.
- **Day Report.** The Day report queries the hour table and displays the exact number of items, such as bytes and connection, that have been recorded by the appliance on an hourly basis over a 24 hour period. This information is gathered from the hour table.

The Week Report and 30 Days Report work similarly to the Hour and Day Reports.

System Status Page

Use the **Reporting > System Status** page to monitor the System Status. This page displays the current status and configuration of the Web Security appliance.

This Section...	Displays
Web Security Appliance Status	<ul style="list-style-type: none"> • System uptime • System resource utilization — CPU usage, RAM usage, and percentage of disk space used for reporting and logging. <p>RAM usage for a system that is working efficiently may be above 90%, because RAM that is not otherwise in use by the system is used by the web object cache. If your system is not experiencing serious performance issues and this value is not stuck at 100%, the system is operating normally.</p> <p>Note Proxy Buffer Memory is one component that uses this RAM.</p>

This Section...	Displays
Proxy Traffic Characteristics	<ul style="list-style-type: none"> • Transactions per second • Bandwidth • Response time • Cache hit rate • Connections
Current Configuration	<p>Web Proxy settings:</p> <ul style="list-style-type: none"> • Web Proxy Status — enabled or disabled. • Deployment Topology. • Web Proxy Mode — forward or transparent. • IP Spoofing — enabled or disabled. <p>L4 Traffic Monitor settings:</p> <ul style="list-style-type: none"> • L4 Traffic Monitor Status — enabled or disabled. • L4 Traffic Monitor Wiring. • L4 Traffic Monitor Action — monitor or block. <p>Web Security Appliance Version Information</p> <p>Hardware information</p>

Related Topics

- [System Capacity Page, page 18-14](#)



Detecting Rogue Traffic on Non-Standard Ports

- [Overview of Detecting Rogue Traffic, page 19-1](#)
- [Configuring the L4 Traffic Monitor, page 19-1](#)
- [List of Known Sites, page 19-2](#)
- [Configuring L4 Traffic Monitor Global Settings, page 19-2](#)
- [Updating L4 Traffic Monitor Anti-Malware Rules, page 19-3](#)
- [Creating a Policy to Detect Rogue Traffic, page 19-3](#)
- [Viewing L4 Traffic Monitor Activity, page 19-4](#)

Overview of Detecting Rogue Traffic

The Web Security appliance has an integrated Layer-4 Traffic Monitor that detects rogue traffic across all network ports and stops malware attempts to bypass port 80. When internal clients are infected with malware and attempt to phone-home across non-standard ports and protocols, the L4 Traffic Monitor prevents phone-home activity from going outside the corporate network. By default, the L4 Traffic Monitor is enabled and set to monitor traffic on all ports. This includes DNS and other services.

The L4 Traffic Monitor uses and maintains its own internal database. This database is continuously updated with matched results for IP addresses and domain names.

Configuring the L4 Traffic Monitor

Before you begin

- Configure the L4 Traffic Monitor inside the firewall.

- Ensure the L4 Traffic Monitor is ‘logically’ connected after the proxy ports and before any device that performs network address translation (NAT) on client IP addresses.

Step 1	Configure the Global Settings	See Configuring L4 Traffic Monitor Global Settings , page 19-2.
Step 2	Create L4 TrafficMonitor Policies	See Creating a Policy to Detect Rogue Traffic , page 19-3.

List of Known Sites

Address	Description
Known allowed	Any IP address or hostname listed in the Allow List property. These addresses appear in the log files as “whitelist” addresses.
Unlisted	Any IP address that is not known to be a malware site nor is a known allowed address. They are not listed on the Allow List, Additional Suspected Malware Addresses properties, or in the L4 Traffic Monitor Database. These addresses do not appear in the log files.
Ambiguous	These appear in the log files as “greylist” addresses and include: <ul style="list-style-type: none"> – Any <i>IP address</i> that is associated with both an unlisted <i>hostname</i> and a known malware <i>hostname</i>. – Any <i>IP address</i> that is associated with both an unlisted <i>hostname</i> and a <i>hostname</i> from the Additional Suspected Malware Addresses property
Known malware	These appear in the log files as “blacklist” addresses and include: <ul style="list-style-type: none"> – Any IP address or hostname that the L4 Traffic Monitor Database determines to be a known malware site and <i>not</i> listed in the Allow List. – Any <i>IP address</i> that is listed in the Additional Suspected Malware Addresses property, <i>not</i> listed in the Allow List and is <i>not</i> ambiguous

Configuring L4 Traffic Monitor Global Settings

- Step 1** Choose **Security Services > L4 Traffic Monitor**.
- Step 2** Click **Edit Global Settings**.
- Step 3** Choose whether or not to enable the L4 Traffic Monitor.
- Step 4** When you enable the L4 Traffic Monitor, choose which ports it should monitor:
 - **All ports.** Monitors all 65535 TCP ports for rogue activity.
 - **All ports except proxy ports.** Monitors all TCP ports except the following ports for rogue activity.

- Ports configured in the “HTTP Ports to Proxy” property on the **Security Services > Web Proxy** page (usually port 80).
- Ports configured in the “Transparent HTTPS Ports to Proxy” property on the **Security Services > HTTPS Proxy** page (usually port 443).

Step 5 Submit and Commit Changes.

Updating L4 Traffic Monitor Anti-Malware Rules

Step 1 Choose **Security Services > L4 Traffic Monitor**.

Step 2 Click **Update Now**.

Creating a Policy to Detect Rogue Traffic

The actions the L4 Traffic Monitor takes depends on the L4 Traffic Monitor policies you configure:

Step 1 Choose **Web Security Manager > L4 Traffic Monitor**.

Step 2 Click **Edit Settings**.

Step 3 On the **Edit L4 Traffic Monitor Policies** page, configure the L4 Traffic Monitor policies:

- a. **Define the Allow List**
- b. Add known good sites to the **Allow List**



Note Do not include the Web Security appliance IP address or hostname to the **Allow List** otherwise the L4 Traffic Monitor does not block any traffic.

- c. Determine which action to perform for **Suspected Malware Addresses**:

Action	Description
Allow	It always allows traffic to and from known allowed and unlisted addresses
Monitor	It monitors traffic under the following circumstances: <ul style="list-style-type: none"> – When the Action for Suspected Malware Addresses option is set to Monitor, it always monitors all traffic that is not to or from a known allowed address. – When the Action for Suspected Malware Addresses option is set to Block, it monitors traffic to and from ambiguous addresses
Block	When the Action for Suspected Malware Addresses option is set to Block, it blocks traffic to and from known malware addresses



Note When you choose to block suspected malware traffic, you can also choose whether or not to always block ambiguous addresses. By default, ambiguous addresses are monitored.



Note If the L4 Traffic Monitor is configured to block, the L4 Traffic Monitor and the Web Proxy must be configured on the same network. Use the **Network > Routes** page to confirm that all clients are accessible on routes that are configured for data traffic.

- d. Define the **Additional Suspected Malware Addresses** properties



Note Adding internal IP addresses to the Additional Suspected Malware Addresses list causes legitimate destination URLs to show up as malware in L4 Traffic Monitor reports. To avoid this do not enter internal IP addresses in the “**Additional Suspected Malware Addresses**” field on the **Web Security Manager > L4 Traffic Monitor Policies** page.

Step 4 **Submit and Commit Changes.**

Related Topics

- [Overview of Detecting Rogue Traffic, page 19-1](#)
- [Valid Formats, page 19-4.](#)

Valid Formats

When you add addresses to the Allow List or Additional Suspected Malware Addresses properties, separate multiple entries with whitespace or commas. You can enter addresses in any of the following formats:

- **IPv4 IP address.** Example: IPv4 format: 10.1.1.0. IPv6 format: 2002:4559:1FE2::4559:1FE2
- **CIDR address.** Example: 10.1.1.0/24.
- **Domain name.** Example: example.com.
- **Hostname.** Example: crm.example.com.

Viewing L4 Traffic Monitor Activity

The S-Series appliance supports several options for generating feature specific reports and interactive displays of summary statistics.

Monitoring Activity and Viewing Summary Statistics

The **Reporting > L4 Traffic Monitor** page provides statistical summaries of monitoring activity. You can use the following displays and reporting tools to view the results of L4 Traffic Monitor activity:

To view...	See...
Client statistics	Reporting > Client Activity
Malware statistics	Reporting > L4 Traffic Monitor
Port statistics	
L4 Traffic Monitor log files	System Administration > Log Subscriptions <ul style="list-style-type: none">• trafmon_errlogs• trafmonlogs

**Note**

If the Web Proxy is configured as a forward proxy and L4 Traffic Monitor is set to monitor all ports, the IP address of the proxy's data port is recorded and displayed as a client IP address in the client activity report on the **Reporting > Client Activity** page. If the Web Proxy is configured as a transparent proxy, enable IP spoofing to correctly record and display the client IP addresses.

L4 Traffic Monitor Log File Entries

The L4 Traffic Monitor log file provides a detailed record of monitoring activity.



Monitor System Activity Through Logs

- [Overview of Logging, page 20-1](#)
- [Tasks for Logging, page 20-2](#)
- [Best Practices for Logging, page 20-2](#)
- [Planning For Logging, page 20-2](#)
- [Adding and Editing Log Subscriptions, page 20-5](#)
- [Viewing Log Files, page 20-9](#)
- [Adding SCP SSH Public Host Keys to the Appliance, page 20-10](#)
- [Troubleshooting Web Proxy Issues Using Logs, page 20-11](#)
- [Access Log Files, page 20-12](#)
- [W3C Compliant Access Log Files, page 20-15](#)
- [Customizing Access Logs, page 20-17](#)
- [Traffic Monitor Log Files, page 20-18](#)
- [Log File Types, page 20-19](#)
- [Log File Fields and Tags, page 20-23](#)

Overview of Logging

The Web Security appliance records its own system and traffic management activities by writing them to log files. Administrators can consult these log files to monitor and troubleshoot the appliance.

The appliance divides different types of activity into different logging types to simplify the task of finding information on specific activities. The majority of these are automatically enabled by default, but some must be manually enabled as required.

You enable and manage log files through log file subscriptions. Subscriptions allow you to define the settings for creating, customizing, and managing log files.

The two main log files typically used by administrators are:

- **Access log.** This records all Web Proxy filtering and scanning activity.
- **Traffic Monitor log.** This records all Layer-4 Traffic Monitor activity.

You can view current and past appliance activity using these and other log types. Reference tables are available to help you interpret log file entries.

Tasks for Logging

Steps	Task	Links to Related Topics and Procedures
1	Plan logging tasks: <ul style="list-style-type: none"> Review the best practices for logging Review logging concepts 	Best Practices for Logging, page 20-2 Planning For Logging, page 20-2
2	Create or change logging subscriptions	Adding and Editing Log Subscriptions, page 20-5
3	View log files	Viewing Log Files, page 20-9
4	Understand Access logs	Access Log Files, page 20-12
5	Understand W3C compliant Access logs	W3C Compliant Access Log Files, page 20-15
7	Customizing Access and W3C Access logs	Customizing Access Logs, page 20-17
7	Understand Traffic Monitor logs	Traffic Monitor Log Files, page 20-18
8	Find log file reference information	Log File Types, page 20-19 Log File Fields and Tags, page 20-23

Best Practices for Logging

- Avoid creating multiple logging subscriptions and using high detail levels when possible, as these can adversely affect system performance.

Planning For Logging

- [Log Types, page 20-2](#)
- [Log Subscriptions, page 20-3](#)
- [Log File Names and Appliance Directory Structure, page 20-3](#)
- [Archiving Log Files Using Rollover, page 20-4](#)
- [Saving Disk Space By Compressing Log Files, page 20-4](#)
- [Reading and Interpreting Log Files, page 20-4](#)

Log Types

A log type defines the range of activity that is recorded in log files of that type. The Web Security appliance provides numerous log types, each of which logs activity related to a specific area.

Two of the main log types that administrators use for normal appliance monitoring are the Access logs and Traffic Monitor logs. Access logs record activity related to client access through the web proxy, including filtering and scanning activity. Traffic Monitor logs record activity related to Layer-4 traffic monitoring.

Access logs are further divided into standard Access logs and W3C compliant access logs. Both can record the same range of activity but do so in different formats. W3C are also more customizable with regard to their content and layout than standard Access logs.

Related Topics

- [Log File Types, page 20-19.](#)
- [Traffic Monitor Log Files, page 20-18.](#)
- [W3C Compliant Access Log Files, page 20-15.](#)
- [Customizing Access Logs, page 20-17.](#)

Log Subscriptions

To enable logging for a log type, you have to create a subscription to that log type. Subscriptions are the collective term for all the settings related to a logging instance. Subscription settings include:

- Rollover settings, which determine when log files are archived.
- Compression settings for archived logs.
- The level of detail written to logs
- Custom field layouts and user-defined fields for Access and W3C compliant logs.
- Retrieval settings for archived logs, which specifies if logs are archive onto a remote server or stored on the appliance.

You can add, edit, or delete log subscriptions and you can create multiple log subscriptions for each type of log file.

Default Log Subscriptions

By default, subscriptions exist on the Web Security appliance for most log types. Some log types related to the web proxy component are not enabled, however. The main web proxy log type, called the “Default Proxy Logs,” is enabled by default and captures basic information on all Web Proxy modules. Each Web Proxy module also has its own log type that you must manually enable as required.

Related Topics

- [Adding and Editing Log Subscriptions, page 20-5.](#)

Log File Names and Appliance Directory Structure

The appliance creates a directory for each log subscription based on the log subscription name. The name of the log file in the directory is composed of the following information:

- Log file name specified in the log subscription
- Timestamp when the log file was started
- A single-character status code, either `.c` (signifying current) or `.s` (signifying saved)

The filename of logs are made using the following formula:

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

**Note**

You should only transfer log files with the saved status.

Related Topics

[Adding and Editing Log Subscriptions, page 20-5.](#)

Archiving Log Files Using Rollover

AsyncOS will periodically close current log files and begin new ones as a means of managing log file size and storage location. This is called log file “rollover”. Based on the retrieval method defined for the log subscription, AsyncOS stores the older log files on the appliance for retrieval or delivers them to an external computer.

AsyncOS rolls over log subscriptions in the following ways:

- **Manually.** The appliance administrator can manually roll over log subscriptions on demand from either the web interface or the CLI.
- **Automatically.** AsyncOS rolls over log subscriptions when a current log file reaches a user-specified limit of maximum file size or maximum time since last rollover. This is configured as part of the subscription settings.

Related Topics

- [Adding and Editing Log Subscriptions, page 20-5.](#)
- [Manually Rolling Over Log Subscriptions, page 20-9.](#)

Saving Disk Space By Compressing Log Files

To save disk space on the Web Security appliance, log subscriptions can compress rolled over log files before storing them on the disk. Only rolled over logs are compressed. The current active log file is not compressed.

Each log subscription has its own log compression setting, so you can choose which log subscriptions to compress. AsyncOS compresses log files using the gzip compression format.

Related Topics

- [Archiving Log Files Using Rollover, page 20-4](#)
- [Adding and Editing Log Subscriptions, page 20-5](#)

Reading and Interpreting Log Files

You can read current log file activity as a means of monitoring and troubleshooting the Web Security appliance. This is done using the appliance interface.

You can also read archived files for a record of past activity. This can be done using the appliance interface if the archived files are stored on the appliance; otherwise they must be read from their external storage location using an appropriate method.

Each item of information in a log file is represented by a field variable. By determining which fields represent which items of information, you can look up the field function and interpret the log file contents. For W3C compliant access logs, the file header lists field names in the order in which they appear in log entries. For standard Access logs, however, you must consult the documentation regarding this log type for information on its field order.

Related Topics

- [Viewing Log Files](#), page 20-9.
- [Interpreting Access Log File Entries](#), page 20-12.
- [Interpreting W3C Access Logs](#), page 20-15.
- [Interpreting Traffic Monitor Logs](#), page 20-19.
- [Log File Fields and Tags](#), page 20-23.

Adding and Editing Log Subscriptions

- Step 1** Choose **System Administration > Log Subscriptions**.
- Step 2** To add a log subscription, click **Add Log Subscription**. Or, to edit a log subscription, click the name of the log file in the Log Name field.
- Step 3** Complete the subscription option.

Option	Description
Log Type	<p>A list of available log file types that you can subscribe to. The other options on the page may change according to log file type you choose.</p> <p>Note The Request Debug Logs log type can only be subscribed to using the CLI and does not appear on this list.</p>
Log Name	The name used to refer to the subscription on the Web Security appliance. This name is also used for the log directory which will store the log files for the subscription.
Rollover by File Size	The maximum file size to which the current log file can grow before it is archived and a new log file started. You must enter a number between 100 kilobytes and 10 gigabytes.
Rollover by Time	<p>The maximum time interval before the current log file is archived and a new log file started. The following interval types are available:</p> <ul style="list-style-type: none"> • None. AsyncOS only performs a rollover when the log file reaches the maximum file size. • Custom Time Interval. AsyncOS performs a rollover after a specified amount of time has passed since the previous rollover. Specify the number of days, hours, minutes, and seconds between rollovers using <i>d</i>, <i>h</i>, <i>m</i>, and <i>s</i> as suffixes. • Daily Rollover. AsyncOS performs a rollover every day at a specified time. Separate multiple times a day using a comma. Use an asterisk (*) for the hour to have rollover occur every hour during the day. You can also use an asterisk to rollover every minute of an hour. • Weekly Rollover. AsyncOS performs a rollover on one or more days of the week at a specified time.
Log Style (Access Logs)	Specifies the log format to use, either Squid, Apache, or Squid Details.

Option	Description
Custom Fields (Access Logs)	<p>Allows you to include custom information in each access log entry.</p> <p>The syntax for entering format specifiers in the Custom Field is as follows:</p> <pre><format_specifier_1> <format_specifier_2> ...</pre> <p>For example: %a %b %E</p> <p>You can add tokens before the format specifiers to display descriptive text in the access log file. For example:</p> <pre>client_IP %a body_bytes %b error_type %E</pre> <p>where <code>client_IP</code> is the description token for log format specifier %a, and so on.</p>
File Name	<p>The name of the log files. Current log files are appended with a <code>.c</code> extension and rolled over log files are appended with the file creation timestamp and a <code>.s</code> extension.</p>
Log Fields (W3C Access Logs)	<p>Allows you to choose the fields you want to include in the W3C access log. Select a field in the Available Fields list, or type a field in the Custom Field box, and click Add.</p> <p>The order the fields appear in the Selected Log Fields list determines the order of fields in the W3C access log file. You can change the order of fields using the Move Up and Move Down buttons. You can remove a field by selecting it in the Selected Log Fields list and clicking Remove.</p> <p>You can enter multiple user defined fields in the Custom Fields box and add them simultaneously as long as each entry is separated by a new line (click Enter) before clicking Add.</p> <p>When you change the log fields included in a W3C log subscription, the log subscription automatically rolls over. This allows the latest version of the log file to include the correct new field headers.</p>
Log Compression	<p>Specifies whether or not rolled over files are compressed. AsyncOS compresses log files using the gzip compression format.</p>
Log Exclusions (Optional) (Access Logs)	<p>Allows you to specify HTTP status codes (4xx or 5xx only) to exclude the associated transactions from an access log or a W3C access log.</p> <p>For example, entering 401 will filter out authentication failure requests that have that transaction number.</p>

Option	Description
Log Level	<p>Specifies the level of detail for log entries. Choose from:</p> <ul style="list-style-type: none"> • Critical. Includes errors only. This is the least detailed setting and is equivalent to the syslog level “Alert.” • Warning. Includes errors and warnings. This log level is equivalent to the syslog level “Warning.” • Information. Includes errors, warnings and additional system operations. This is the default detail level and is equivalent to the syslog level “Info.” • Debug. Includes data useful for debugging system problems. Use the Debug log level when you are trying to discover the cause of an error. Use this setting temporarily, and then return to the default level. This log level is equivalent to the syslog level “Debug.” • Trace. This is the most detailed setting. This level includes a complete record of system operations and activity. The Trace log level is recommended only for developers. Using this level causes a serious degradation of system performance and is not recommended. This log level is equivalent to the syslog level “Debug.” <p>Note More detailed settings create larger log files and have a greater impact on system performance.</p>
Retrieval Method	<p>Specifies where rolled over log files are stored and how they are retrieved for reading. See below for descriptions of the available methods.</p>
Retrieval Method: FTP on Appliance	<p>The FTP on Appliance method (equivalent to FTP Poll) requires a remote FTP client accessing the appliance to retrieve log files using an admin or operator user’s username and password.</p> <p>When you choose this method, you must enter the maximum number of log files to store on the appliance. When the maximum number is reached, the system deletes the oldest file.</p> <p>This is the default retrieval method.</p>
Retrieval Method: FTP on Remote Server	<p>The FTP on Remote Server method (equivalent to FTP Push) periodically pushes log files to an FTP server on a remote computer.</p> <p>When you choose this method, you must enter the following information:</p> <ul style="list-style-type: none"> • FTP server hostname • Directory on FTP server to store the log file • Username and password of a user that has permission to connect to the FTP server <p>Note AsyncOS for Web only supports passive mode for remote FTP servers. It cannot push log files to an FTP server in active mode.</p>

Option	Description
Retrieval Method: SCP on Remote Server	<p>The SCP on Remote Server method (equivalent to SCP Push) periodically pushes log files using the secure copy protocol to a remote SCP server. This method requires an SSH SCP server on a remote computer using the SSH2 protocol. The subscription requires a user name, SSH key, and destination directory on the remote computer. Log files are transferred based on a rollover schedule set by you.</p> <p>When you choose this method, you must enter the following information:</p> <ul style="list-style-type: none"> • SCP server hostname • Directory on SCP server to store the log file • Username of a user that has permission to connect to the SCP server
Retrieval Method: Syslog Push	<p>The Syslog Push method sends log messages to a remote syslog server on port 514. This method conforms to RFC 3164.</p> <p>When you choose this method, you must enter the following information:</p> <ul style="list-style-type: none"> • Syslog server hostname • Protocol to use for transmission, either UDP or TCP • Facility to use with the log <p>You can only choose syslog for text-based logs.</p> <p>Syslog messages greater than 1024 bytes are truncated. Access logs and W3C access logs with many custom variables, especially of variable length, might exceed the 1024 byte limit.</p>

Step 4 Submit and commit your changes.

Step 5 If you chose SCP as the retrieval method, the appliance displays an SSH key to you must place on the SCP server host.

Related Topics

- [Planning For Logging, page 20-2.](#)

Deleting a Log Subscription

Step 1 Choose **System Administration > Log Subscriptions**.

Step 2 Click the icon under the Delete column for the log subscription you want to delete.

Step 3 Submit and commit your changes.

Related Topics

- [Log Subscriptions, page 20-3.](#)

Manually Rolling Over Log Subscriptions

-
- Step 1** Choose System Administration > Log Subscriptions.
 - Step 2** Check the checkbox in the Rollover column of the log subscriptions you wish to roll over, or check the **All** checkbox to select all the subscriptions.
 - Step 3** Click **Rollover Now** to roll over the selected logs.
-

Related Topics

- [Archiving Log Files Using Rollover, page 20-4.](#)
- [Adding and Editing Log Subscriptions, page 20-5.](#)

Viewing Log Files

You can use the Web interface or Command Line Interface to view log files that are currently being written to. The CLI allows you to view current log activity in real time, while you must refresh the Web interface to display the new entries (though this may vary with different browsers).

You can also use the Web interface to view rolled over log files, if the files are stored on the appliance. Otherwise, you must use the appropriate means to access the external storage location and read the logs.

Viewing Log Files Using the Web Interface

-
- Step 1** Choose **Administration > Log Subscriptions**.
 - Step 2** Click the name of the log subscription in the Log Files column of the list of log subscriptions.
 - Step 3** When prompted, enter the administrator's username and password for accessing the appliance.
 - Step 4** When logged in, click one of the log files to view it in your browser or to save it to disk.



Note If a log subscription is compressed, you must download it before you can decompress and open it.

Viewing Log Files Using the Command Line Interface

-
- Step 1** Access the CLI.
 - Step 2** Enter the `tail` command:

```
example.com> tail
```

```
Currently configured logs:
```

```

1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
3. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
4. "bs_access_test" Type: "Access Logs" Retrieval: FTP Poll
[...Output truncated...]
34. "uds_logs" Type: "UDS Logs" Retrieval: FTP Poll
35. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
36. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
37. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
38. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
39. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP
Poll
Enter the number of the log you wish to tail.
[]>

```

Step 3 Enter a number corresponding to the log file you wish to view

```

[]> 1

Press Ctrl-C to stop.
#Version: 1.0
#Date: yyyy-mm-dd hh:mm:ss
#System: 172.x.x.x - example.com
#Software: AsyncOS for Web 8.0.0-xxx
#Fields: %t %e %a %w/%h %s %2r %A %H/%d %c %D %Xr
%?BLOCK_SUSPECT_USER_AGENT,MONITOR_SUSPECT_USER_AGENT?%<User-Agent:!!%-%.

```

The current log file contents are displayed and the screen updates with new log activity as it occurs.

Step 4 Press **CTRL-C** when finished, to stop the trace.

Related Topics

- [Interpreting Access Log File Entries, page 20-12.](#)
- [Interpreting W3C Access Logs, page 20-15.](#)
- [Interpreting Traffic Monitor Logs, page 20-19.](#)

Adding SCP SSH Public Host Keys to the Appliance

If using Secure Copy Protocol (SCP) to push log files to another server from the Web Security appliance, you need to add the remote server's SSH public host key to the appliance. SSH servers have a pair of host keys, one private and one public. The private host key resides on the SSH server and cannot be read by remote machines. The public host key is distributed to any client machine that needs to interact with the SSH server.

Step 1 Access the CLI.

Step 2 Use the `logconfig -> hostkeyconfig` command to access the required area.

Step 3 Use the commands below to perform the required tasks:

Command	Description
New	Add a new key.
Host	Display system host keys. This is the value to place in the remote system's 'known_hosts' file.
Fingerprint	Display system host key fingerprints.
User	Displays the public key of the system account that pushes the logs to the remote machine. This is the same key that is displayed when setting up an SCP push subscription. This is the value to place in the remote system's 'authorized_keys' file.

Step 4 Commit your changes.

Related Topics

- [Adding and Editing Log Subscriptions, page 20-5.](#)

Troubleshooting Web Proxy Issues Using Logs

By default, the Web Security appliance has one log subscription created for Web Proxy logging messages, called the “Default Proxy Logs.” This captures basic information on all Web Proxy modules. The appliance also includes log file types for each Web Proxy module so you can read more specific debug information for each module without cluttering up the Default Proxy Logs.

Follow the steps below to troubleshoot Web Proxy issues using the various logs available.

Step 1 Read the Default Proxy Logs.

Step 2 If you see an entry that might related to the issue but does not have enough information to resolve it, create a log subscription for the relevant specific Web Proxy module. The following Web Proxy module logs types are available:

Access Control Engine Logs	Logging Framework Logs
AVC Engine Framework Logs	McAfee Integration Framework Logs
Configuration Logs	Memory Manager Logs
Connection Management Logs	Miscellaneous Proxy Modules Logs
Data Security Module Logs	Request Debug Logs
DCA Engine Framework Logs	SNMP Module Logs
Disk Manager Logs	Sophos Integration Framework Logs
FireAMP	WBRS Framework Logs
FTP Proxy Logs	WCCP Module Logs
HTTPS Logs	Webcat Integration Framework Logs
License Module Logs	Webroot Integration Framework Logs

- Step 3** Recreate the issue and read the new Web Proxy module log for relevant entries.
- Step 4** Repeat as required with other Web Proxy module logs.
- Step 5** Remove subscriptions that are no longer required.

Related Topics

- [Adding and Editing Log Subscriptions, page 20-5.](#)

Access Log Files

Access log files provides a descriptive record of all Web Proxy filtering and scanning activity. Access log file entries display a record of how the appliance handled each transaction.

**Note**

The W3C access log also records all Web Proxy filtering and scanning activity, but in a format that is W3C compliant.

Interpreting Access Log File Entries

The following text is an example access log file entry for a single transaction:

```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain
DEFAULT_CASE_11-AccessOrDecryptionPolicy-Identity-OutboundMalwareScanningPolicy-DataSecurityPolicy-ExternalDLPPolicy-RoutingPolicy
<IW_comp,6.9,-,-,"-",-,-,-,-,"-",-,-,-,-,"-",-,-,-,-,"-",-,-,-,-,IW_comp,-,"-","-","Unknown","Unknown",-,"-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"> -
```

Each item of information in this example corresponds to a log file format specifier. Use the following table to match the information items to their format specifiers:

Position	Field Value	Format Specifier
1	1278096903.150	%t
2	97	%e
3	172.xx.xx.xx	%a
4	TCP_MISS	%w
5	200	%h
6	8187	%s
7	GET http://my.site.com/	%2r
8	-	%A
9	DIRECT	%H
10	my.site.com	%d
11	text/plain	%c

Position	Field Value	Format Specifier
12	DEFAULT_CASE_11	%D
13	AccessOrDecryptionPolicy	N/A (Part of &D)
14	Identity	N/A (Part of &D)
15	OutboundMalwareScanningPolicy	N/A (Part of &D)
16	DataSecurityPolicy	N/A (Part of &D)
17	ExternalDLPPolicy	N/A (Part of &D)
18	RoutingPolicy	N/A (Part of &D)
19	<IW_comp,6.9,-,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-",-,-,"-",-,-, IW_comp,-,-,"-",-,"Unknown","Unknown","-","-","-","198.34,0,-,[Local],"-","37","W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e">	%Xr
20	-	%%?BLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?%%<User-Agent:%%!%-%.>

Refer to [Log File Fields and Tags, page 20-23](#) for a description of each format specifier's function.

Interpreting Access Log Scanning Verdict Entries

The access log file entries aggregate and display the results of the various scanning engines, such as URL filtering, Web Reputation filtering, and anti-malware scanning. The appliance displays this information in angled brackets at the end of each access log entry.

The following text is the scanning verdict information from an access log file entry. In this example, the Webroot scanning engine found the malware:

```
<IW_infr,ns,24,"Trojan-Phisher-Gamec",0,354385,12559,-,-,-,-,-,"-",-,-,-,-,"-",-,-,-,-,"-",-,-,-, IW_infr,-,"Trojan Phisher",-,"Unknown","Unknown",-,-,"-",-,"489.73,0,-,[Local],"-","37","W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e">
```



Note

For an example of a whole access log file entry, see [Traffic Monitor Log Files, page 20-18](#).

Each item of information in this example corresponds to a log file format specifier as shown in the following table:

Position	Field Value	Format Specifier
1	IW_infr	%XC
2	ns	%XW
3	24	%Xv
4	"Trojan-Phisher-Gamec"	"%Xn"

Position	Field Value	Format Specifier
5	0	%Xt
6	354385	%Xs
7	12559	%Xi
8	-	%Xd
9	" - "	"%Xe"
10	-	%Xf
11	-	%Xg
12	-	%Xh
13	" - "	"%Xj"
14	-	%XY
15	-	%Xx
16	" - "	"%Xy"
17	" - "	"%Xz"
18	-	%Xl
19	-	%Xp
20	IW_infr	%XQ
21	-	%XA
22	"Trojan Phisher"	"%XZ"
23	" - "	"%Xk"
24	"Unknown"	"%XO"
25	"Unknown"	"%Xu"
26	" - "	"%Xb"
27	" - "	"%XS"
28	489.73	%XB
29	0	%XT
30	[Local]	%l
31	" - "	"%X3"
32	" - "	"%X4"
33	37	%X#1#
34	"W32.CiscoTestVector"	%X#2#
35	33	%X#3#
36	0	%X#4#
37	"WSA-INFECTED-FILE.pdf"	%X#5#
38	"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"	%X#6#

Refer to [Log File Fields and Tags](#), page 20-23 for a description of each format specifier's function.

Related Topics

- [Adding and Editing Log Subscriptions, page 20-5](#)
- [Customizing Access Logs, page 20-17.](#)
- [W3C Compliant Access Log Files, page 20-15](#)
- [Viewing Log Files, page 20-9](#)
- [Log File Fields and Tags, page 20-23](#)

W3C Compliant Access Log Files

The Web Security appliance provides two different log types for recording Web Proxy transaction information: access logs and W3C access logs. W3C access logs are W3C compliant, and record transaction history in the W3C Extended Log File (ELF) Format.

- [W3C Field Types, page 20-15](#)
- [Interpreting W3C Access Logs, page 20-15](#)

W3C Field Types

When defining a W3C access log subscription, you must choose which log fields to include, such as the ACL decision tag or the client IP address. You can include one of the following types of log fields:

- **Predefined.** The web interface includes a list of fields from which you can choose.
- **User defined.** You can type a log field that is not included in the predefined list.

Interpreting W3C Access Logs

Consider the following rules and guidelines when interpreting W3C access logs:

- Administrators decide what data is recorded in each W3C access log subscription; therefore, W3C access logs have no set field format.
- W3C logs are self-describing. The file format (list of fields) is defined in a header at the start of each log file.
- Fields in the W3C access logs are separated by a white space.
- If a field contains no data for a particular entry, a hyphen (-) is included in the log file instead.
- Each line in the W3C access log file relates to one transaction, and each line is terminated by a LF sequence.
- [W3C Log File Headers, page 20-15](#)
- [W3C Field Prefixes, page 20-16](#)

W3C Log File Headers

Each W3C log file contains header text at the beginning of the file. Each line starts with the # character and provides information about the Web Security appliance that created the log file. The W3C log file headers also include the file format (list of fields), making the log file self-describing.

The following table describes the header fields listed at the beginning of each W3C log file.

Header Field	Description
Version	The version of the W3C ELF format used.
Date	The date and time at which the header (and log file) was created.
System	The Web Security appliance that generated the log file in the format “Management_IP - Management_hostname.”
Software	The Software which generated these logs
Fields	The fields recorded in the log

Example W3C log file:

```
#Version: 1.0
#Date: 2009-06-15 13:55:20
#System: 10.1.1.1 - wsa.qa
#Software: AsyncOS for Web 6.3.0
#Fields: timestamp x-elapsed-time c-ip x-resultcode-httpstatus sc-bytes cs-method
cs-url cs-username x-hierarchy-origin cs-mime-type x-acltag x-result-code
x-suspect-user-agent
```

W3C Field Prefixes

Most W3C log field names include a prefix that identifies from which header a value comes, such as the client or server. Log fields without a prefix reference values that are independent of the computers involved in the transaction. The following table describes the W3C log fields prefixes.

Prefix Header	Description
c	Client
s	Server
cs	Client to server
sc	Server to client
x	Application specific identifier.

For example, the W3C log field “cs-method” refers to the method in the request sent by the client to the server, and “c-ip” refers to the client’s IP address.

Related Topics

- [Adding and Editing Log Subscriptions, page 20-5.](#)
- [For information on user defined fields, see Access Log User Defined Fields, page 20-17., page 20-17.](#)
- [Traffic Monitor Log Files, page 20-18.](#)
- [Log File Fields and Tags, page 20-23.](#)
- [Viewing Log Files, page 20-9.](#)

Customizing Access Logs

You can customize regular and W3C access logs to include many different fields to capture comprehensive information about web traffic within the network using predefined fields or user defined fields.

Related Topics

- For a list of predefined fields, see [Log File Fields and Tags, page 20-23](#).
- For information on user defined fields, see [Access Log User Defined Fields, page 20-17](#).

Access Log User Defined Fields

If the list of predefined Access log and W3C log fields does not include all header information you want to log from HTTP/HTTPS transactions, you can type a user defined log field in the Custom Fields text box when you configure the access and W3C log subscriptions.

Custom log fields can be any data from any header sent from the client or the server. If a request or response does not include the header added to the log subscription, the log file includes a hyphen as the log field value.

The following table defines the syntax to use for access and W3C logs:

Header Type	Access Log Format Specifier Syntax	W3C Log Custom Field Syntax
Header from the client application	<i>%<ClientHeaderName:</i>	<i>cs(<ClientHeaderName)</i>
Header from the server	<i>%<ServerHeaderName:</i>	<i>sc(<ServerHeaderName)</i>

For example, if you want to log the If-Modified-Since header value in client requests, enter the following text in the Custom Fields box for a W3C log subscription:

```
cs(If-Modified-Since)
```

Related Topics

- [Customizing Regular Access Logs, page 20-17](#).
- [Customizing W3C Access Logs, page 20-18](#).

Customizing Regular Access Logs

-
- Step 1** Choose System Administration > Log Subscriptions.
- Step 2** Click the access log file name to edit the access log subscription.
- Step 3** Enter the required format specifiers in the Custom Field.

The syntax for entering format specifiers in the Custom Field is as follows:

```
<format_specifier_1> <format_specifier_2> ...
```

For example: %a %b %E

You can add tokens before the format specifiers to display descriptive text in the access log file. For example:

```
client_IP %a body_bytes %b error_type %E
```

where `client_IP` is the description token for log format specifier `%a`, and so on.



Note You can create a custom field for any header in a client request or a server response.

Step 4 Submit and commit your changes.

Related Topics

- [Access Log Files, page 20-12.](#)
- [Log File Fields and Tags, page 20-23.](#)
- [Access Log User Defined Fields, page 20-17.](#)

Customizing W3C Access Logs

Step 1 Choose **System Administration > Log Subscriptions**

Step 2 Click the W3C log file name to edit the W3C log subscription.

Step 3 Type a field in the Custom Field box, and click **Add**.

The order the fields appear in the Selected Log Fields list determines the order of fields in the W3C access log file. You can change the order of fields using the **Move Up** and **Move Down** buttons. You can remove a field by selecting it in the Selected Log Fields list and clicking **Remove**.

You can enter multiple user defined fields in the Custom Fields box and add them simultaneously as long as each entry is separated by a new line (click Enter) before clicking **Add**.

When you change the log fields included in a W3C log subscription, the log subscription automatically rolls over. This allows the latest version of the log file to include the correct new field headers.



Note You can create a custom field for any header in a client request or a server response.

Step 4 Submit and commit your changes.

Related Topics

- [W3C Compliant Access Log Files, page 20-15.](#)
- [Log File Fields and Tags, page 20-23.](#)
- [Access Log User Defined Fields, page 20-17.](#)

Traffic Monitor Log Files

Layer-4 Traffic Monitor log files provides a detailed record of Layer-4 monitoring activity. You can view Layer-4 Traffic Monitor log file entries to track updates to firewall block lists and firewall allow lists.

Interpreting Traffic Monitor Logs

Use the examples below to interpret the various entry types contains in Traffic Monitor Logs.

Example 1

172.xx.xx.xx discovered for blocksite.net (blocksite.net) added to firewall block list.

In this example, where a match becomes a block list firewall entry. The Layer-4 Traffic Monitor matched an IP address to a domain name in the block list based on a DNS request which passed through the appliance. The IP address is then entered into the block list for the firewall.

Example 2

172.xx.xx.xx discovered for www.allowsite.com (www.allowsite.com) added to firewall allow list.

In this example, a match becomes an allow list firewall entry. The Layer-4 Traffic Monitor matched a domain name entry and added it to the appliance allow list. The IP address is then entered into the allow list for the firewall.

Example 3

Firewall noted data from 172.xx.xx.xx to 209.xx.xx.xx (allowsite.net):80.

In this example, the Layer-4 Traffic Monitor logs a record of data that passed between an internal IP address and an external IP address which is on the block list. Also, the Layer-4 Traffic Monitor is set to monitor, not block.

Related Topics

- [Viewing Log Files, page 20-9.](#)

Log File Types

The log file type indicates what information is recorded in the generated log, such as web traffic or system data. The Web Security appliance has log subscriptions for most log file types by default, with the exception of Web Proxy troubleshooting logs.

The following table describes the Web Security appliance log file types.

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
Access Control Engine Logs	Records messages related to the Web Proxy ACL (access control list) evaluation engine.	No	No
AMP Engine Logs	Records information about file reputation scanning and file analysis (Advanced Malware Protection.) See also Log Files .	Yes	Yes
Access Logs	Records Web Proxy client history.	Yes	Yes
Authentication Framework Logs	Records authentication history and messages.	No	Yes
AVC Engine Framework Logs	Records messages related to communication between the Web Proxy and the AVC engine.	No	No
AVC Engine Logs	Records debug messages from the AVC engine.	Yes	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
CLI Audit Logs	Records a historical audit of command line interface activity.	Yes	Yes
Configuration Logs	Records messages related to the Web Proxy configuration management system.	No	No
Connection Management Logs	Records messages related to the Web Proxy connection management system.	No	No
Data Security Logs	Records client history for upload requests that are evaluated by the Cisco Data Security Filters.	Yes	Yes
Data Security Module Logs	Records messages related to the Cisco Data Security Filters.	No	No
DCA Engine Framework Logs (Dynamic Content Analysis)	Records messages related to communication between the Web Proxy and the Cisco Web Usage Controls Dynamic Content Analysis engine.	No	No
DCA Engine Logs (Dynamic Content Analysis)	Records messages related to the Cisco Web Usage Controls Dynamic Content Analysis engine.	Yes	Yes
Default Proxy Logs	Records errors related to the Web Proxy. This is the most basic of all Web Proxy related logs. To troubleshoot more specific aspects related to the Web Proxy, create a log subscription for the applicable Web Proxy module.	Yes	Yes
Disk Manager Logs	Records Web Proxy messages related to writing to the cache on disk.	No	No
External Authentication Logs	Records messages related to using the external authentication feature, such as communication success or failure with the external authentication server. Even with external authentication is disabled, this log contains messages about local users successfully or failing logging in.	No	Yes
Feedback Logs	Records the web users reporting misclassified pages.	Yes	Yes
FTP Proxy Logs	Records error and warning messages related to the FTP Proxy.	No	No
FTP Server Logs	Records all files uploaded to and downloaded from the Web Security appliance using FTP.	Yes	Yes
GUI Logs (Graphical User Interface)	Records history of page refreshes in the web interface. GUI logs also include information about SMTP transactions, for example information about scheduled reports emailed from the appliance.	Yes	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
Haystack Logs	Haystack logs record web transaction tracking data processing.	Yes	Yes
HTTPS Logs	Records Web Proxy messages specific to the HTTPS Proxy (when the HTTPS Proxy is enabled).	No	No
License Module Logs	Records messages related to the Web Proxy's license and feature key handling system.	No	No
Logging Framework Logs	Records messages related to the Web Proxy's logging system.	No	No
Logging Logs	Records errors related to log management.	Yes	Yes
McAfee Integration Framework Logs	Records messages related to communication between the Web Proxy and the McAfee scanning engine.	No	No
McAfee Logs	Records the status of anti-malware scanning activity from the McAfee scanning engine.	Yes	Yes
Memory Manager Logs	Records Web Proxy messages related to managing all memory including the in-memory cache for the Web Proxy process.	No	No
Miscellaneous Proxy Modules Logs	Records Web Proxy messages that are mostly used by developers or customer support.	No	No
AnyConnect Secure Mobility Daemon Logs	Records the interaction between the Web Security appliance and the AnyConnect client, including the status check.	Yes	Yes
NTP Logs (Network Time Protocol)	Records changes to the system time made by the Network Time Protocol.	Yes	Yes
PAC File Hosting Daemon Logs	Records proxy auto-config (PAC) file usage by clients.	Yes	Yes
Proxy Bypass Logs	Records transactions that bypass the Web Proxy.	No	Yes
Reporting Logs	Records a history of report generation.	Yes	Yes
Reporting Query Logs	Records errors related to report generation.	Yes	Yes
Request Debug Logs	Records very detailed debug information on a specific HTTP transaction from all Web Proxy module log types. You might want to create this log subscription to troubleshoot a proxy issue with a particular transaction without creating all other proxy log subscriptions. Note: You can create this log subscription in the CLI only.	No	No
Auth Logs	Records messages related to the Access Control feature.	Yes	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
SHD Logs (System Health Daemon)	Records a history of the health of system services and a history of unexpected daemon restarts.	Yes	Yes
SNMP Logs	Records debug messages related to the SNMP network management engine.	Yes	Yes
SNMP Module Logs	Records Web Proxy messages related to interacting with the SNMP monitoring system.	No	No
Sophos Integration Framework Logs	Records messages related to communication between the Web Proxy and the Sophos scanning engine.	No	No
Sophos Logs	Records the status of anti-malware scanning activity from the Sophos scanning engine.	Yes	Yes
Status Logs	Records information related to the system, such as feature key downloads.	Yes	Yes
System Logs	Records DNS, error, and commit activity.	Yes	Yes
Traffic Monitor Error Logs	Records L4TM interface and capture errors.	Yes	Yes
Traffic Monitor Logs	Records sites added to the L4TM block and allow lists.	No	Yes
UDS Logs (User Discovery Service)	Records data about how the Web Proxy discovers the user name without doing actual authentication. It includes information about interacting with the Cisco adaptive security appliance for the Secure Mobility as well as integrating with the Novell eDirectory server for transparent user identification.	Yes	Yes
Updater Logs	Records a history of WBRs and other updates.	Yes	Yes
W3C Logs	Records Web Proxy client history in a W3C compliant format. For more information, see W3C Compliant Access Log Files, page 20-15 .	Yes	No
WBNP Logs (SensorBase Network Participation)	Records a history of Cisco SensorBase Network participation uploads to the SensorBase network.	No	Yes
WBRs Framework Logs (Web Reputation Score)	Records messages related to communication between the Web Proxy and the Web Reputation Filters.	No	No
WCCP Module Logs	Records Web Proxy messages related to implementing WCCP.	No	No

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
Webcat Integration Framework Logs	Records messages related to communication between the Web Proxy and the URL filtering engine associated with Cisco Web Usage Controls.	No	No
Webroot Integration Framework Logs	Records messages related to communication between the Web Proxy and the Webroot scanning engine.	No	No
Webroot Logs	Records the status of anti-malware scanning activity from the Webroot scanning engine.	Yes	Yes
Welcome Page Acknowledgement Logs	Records a history of web clients who click the Accept button on the end-user acknowledgement page.	Yes	Yes

Related Topics

- [Planning For Logging, page 20-2.](#)
- [Adding and Editing Log Subscriptions, page 20-5.](#)

Log File Fields and Tags

- [Access and W3C Log File Fields, page 20-23](#)
- [Transaction Result Codes, page 20-33](#)
- [ACL Decision Tags, page 20-33](#)
- [Malware Scanning Verdict Values, page 20-37](#)

Access and W3C Log File Fields

Log files use variables to represent the individual items of information that make up each log file entry. These variables are called format specifiers in Access logs and log fields in W3C logs and each format specifier has a corresponding log field.

The following table describes these variables:

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%:<1	x-p2s-first-byte-time	The time it takes from the moment the Web Proxy starts connecting to the server to the time it is first able to write to the server. If the Web Proxy has to connect to several servers to complete the transaction, it is the sum of those times.
%:<a	x-p2p-auth-wait-time	Wait-time to receive the response from the Web Proxy authentication process, after the Web Proxy sent the request.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%:<b	x-p2s-body-time	Wait-time to write request body to server after header
%:<d	x-p2p-dns-wait-time	Time taken by the Web Proxy to send the DNS request to the Web Proxy DNS process.
%:<h	x-p2s-header-time	Wait-time to write request header to server after first byte
%:<r	x-p2p-reputation-wait-time	Wait-time to receive the response from the Web Reputation Filters, after the Web Proxy sent the request.
%:<s	x-p2p-asw-req-wait-time	Wait-time to receive the verdict from the Web Proxy anti-spyware process, after the Web Proxy sent the request.
%:>1	x-s2p-first-byte-time	Wait-time for first response byte from server
%:>a	x-p2p-auth-svc-time	Wait-time to receive the response from the Web Proxy authentication process, including the time required for the Web Proxy to send the request.
%:>b	x-s2p-body-time	Wait-time for complete response body after header received
%:>c	x-p2p-fetch-time	Time required for the Web Proxy to read a response from the disk cache.
%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy DNS process to send back a DNS result to the Web Proxy.
%:>h	x-s2p-header-time	Wait-time for server header after first response byte
%:>r	x-p2p-reputation-svc-time	Wait-time to receive the verdict from the Web Reputation Filters, including the time required for the Web Proxy to send the request.
%:>s	x-p2p-asw-req-svc-time	Wait-time to receive the verdict from the Web Proxy anti-spyware process, including the time required for the Web Proxy to send the request.
%:1<	x-c2p-first-byte-time	Wait-time for first request byte from new client connection
%:1>	x-p2c-first-byte-time	Wait-time for first byte written to client
%:A<	x-p2p-avc-svc-time	Wait-time to receive the response from the AVC process, including the time required for the Web Proxy to send the request.
%:A>	x-p2p-avc-wait-time	Wait-time to receive the response from the AVC process, after the Web Proxy sent the request.
%:b<	x-c2p-body-time	Wait-time for complete client body

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%.b>	x-p2c-body-time	Wait-time for complete body written to client
%.C<	x-p2p-dca-resp-svc-time	Wait-time to receive the verdict from the Dynamic Content Analysis engine, including the time required for the Web Proxy to send the request.
%.C>	x-p2p-dca-resp-wait-time	Wait-time to receive the response from the Dynamic Content Analysis engine, after the Web Proxy sent the request.
%.h<	x-c2p-header-time	Wait-time for complete client header after first byte
%.h>	x-s2p-header-time	Wait-time for complete header written to client
%.m<	x-p2p-mcafee-resp-svc-time	Wait-time to receive the verdict from the McAfee scanning engine, including the time required for the Web Proxy to send the request.
%.m>	x-p2p-mcafee-resp-wait-time	Wait-time to receive the response from the McAfee scanning engine, after the Web Proxy sent the request.
%.p<	x-p2p-sophos-resp-svc-time	Wait-time to receive the verdict from the Sophos scanning engine, including the time required for the Web Proxy to send the request.
%.p>	x-p2p-sophos-resp-wait-time	Wait-time to receive the response from the Sophos scanning engine, after the Web Proxy sent the request.
%.w<	x-p2p-webroot-resp-svc-time	Wait-time to receive the verdict from the Webroot scanning engine, including the time required for the Web Proxy to send the request.
%.w>	x-p2p-webroot-resp-wait-time	Wait-time to receive the response from the Webroot scanning engine, after the Web Proxy sent the request.
%.?BLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?%<User-Agent:!!%-%.	x-suspect-user-agent	Suspect user agent, if applicable. If the Web Proxy determines the user agent is suspect, it will log the user agent in this field. Otherwise, it logs a hyphen. This field is written with double-quotes in the access logs.
%<Referer:	cs(Referer)	Referer
%>Server:	sc(Server)	Server header in the response
%a	c-ip	Client IP Address
%A	cs-username	Authenticated user name. This field is written with double-quotes in the access logs.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%b	sc-body-size	Bytes sent to the client from the Web Proxy for the body content.
%B	bytes	Total bytes used (request size + response size, which is %q + %s)
%c	cs-mime-type	Response body MIME type. This field is written with double-quotes in the access logs.
%C	cs(Cookie)	Cookie header. This field is written with double-quotes in the access logs.
%d	s-hostname	Data source or server IP address
%D	x-acltag	ACL decision tag
%e	x-elapsed-time	<p>Elapsed time in milliseconds.</p> <p>For TCP traffic, this is the time elapsed between the opening and closing of the HTTP connection.</p> <p>For UDP traffic, this is the time elapsed between the sending of the first datagram and the time at which the last datagram can be accepted. A large elapsed time value for UDP traffic may indicate that a large timeout value and a long-lived UDP association allowed datagrams to be accepted longer than necessary.</p>
%E	x-error-code	Error code number that may help Customer Support troubleshoot the reason for a failed transaction.(
%f	cs(X-Forwarded-For)	X-Forwarded-For header
%F	c-port	Client source port
%g	cs-auth-group	Authorized group names. This field is written with double-quotes in the access logs.
%h	sc-http-status	HTTP response code
%H	s-hierarchy	Hierarchy retrieval
%i	x-icap-server	IP address of the last ICAP server contacted while processing the request.
%I	x-transaction-id	Transaction ID

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%j	DCF	<p>Do not cache response code; DCF flags.</p> <p>Response code descriptions:</p> <ul style="list-style-type: none"> • Response code based on client request: <ul style="list-style-type: none"> - 1 = Request had "no-cache" header. - 2 = Caching is not authorized for the request. - 4 = Request is missing the 'Variant' header. - 8 = Username or password needed for user request. - 20 = Response for specified HTTP method. • Response code based on response received by the appliance: <ul style="list-style-type: none"> - 40 = Response contains 'Cache-Control: private' header. - 80 = Response contains 'Cache-Control: no-store' header. - 100 = Response indicates that request was a query. - 200 = Response has a small "Expires" value (expires soon). - 400 = Response does not have "Last Modified" header. - 1000 = Response expires immediately. - 2000 = Response file is too big to cache. - 20000 = New copy of file exists. - 40000 = Response has bad/invalid values in "Vary" header. - 80000 = Response requires Setting of cookies. - 100000 = Non-cacheable HTTP STATUS Code. - 200000 = Object received by appliance was incomplete (based on size). - 800000 = Response trailers indicate no caching. - 1000000 = Response requires re-write.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%k	s-ip	Data source IP address (server IP address)
%l	user-type	Type of user, either local or remote.
%L	x-local_time	Request local time in human readable format: DD/MMM/YYYY : hh:mm:ss +nnnn. This field is written with double-quotes in the access logs.
%m	cs-auth-mechanism	The authentication mechanism used on the transaction. Possible values are: <ul style="list-style-type: none"> • BASIC. The user name was authenticated using the Basic authentication scheme. • NTLMSSP. The user name was authenticated using the NTLMSSP authentication scheme. • SSO_TUI. The user name was obtained by matching the client IP address to an authenticated user name using transparent user identification. • SSO_ASA. The user is a remote user and the user name was obtained from a Cisco ASA using the Secure Mobility. • FORM_AUTH. The user entered authentication credentials in a form in the web browser when accessing a application. • GUEST. The user failed authentication and instead was granted guest access.
%M	CMF	Cache miss flags, CMF flags
%N	s-computerName	Server name or destination hostname. This field is written with double-quotes in the access logs.
%p	s-port	Destination port number
%P	cs-version	Protocol
%q	cs-bytes	Request size (headers + body)
%r	x-req-first-line	Request first line - request method, URI.
%s	sc-bytes	Response size (header + body)
%t	timestamp	Timestamp in UNIX epoch Note: If you want to use a third party log analyzer tool to read and parse the W3C access logs, you might need to include the “timestamp” field. Most log analyzers only understand time in the format provided by this field.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%u	cs(User-Agent)	User agent. This field is written with double-quotes in the access logs.
%U	cs-uri	Request URI
%v	date	Date in YYYY-MM-DD
%V	time	Time in HH:MM:SS
%w	sc-result-code	Result code For example: TCP_MISS, TCP_HIT
%W	sc-result-code-denial	Result code denial
%x	x-latency	Latency
%X0	x-resp-dvs-scanverdict	Unified response-side anti-malware scanning verdict that provides the <i>malware category number</i> independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning. This field is written with double-quotes in the access logs.
%X1	x-resp-dvs-threat-name	Unified response-side anti-malware scanning verdict that provides the <i>malware threat name</i> independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning. This field is written with double-quotes in the access logs.
%X2	x-req-dvs-scanverdict	Request side DVS Scan verdict
%X3	x-req-dvs-verdictname	Request side DVS verdict name
%X4	x-req-dvs-threat-name	Request side DVS threat name
%X6	x-as-malware-threat-name	Indicates whether or not Adaptive Scanning blocked the transaction without invoke any anti-malware scanning engine. The possible values are: <ul style="list-style-type: none"> • 1. Transaction was blocked. • 0. Transaction was not blocked. This variable is included in the scanning verdict information (in the angled brackets at the end of each access log entry).
%XA	x-webcat-resp-code-abbr	The URL category verdict determined during response-side scanning, abbreviated. Applies to the Cisco Web Usage Controls URL filtering engine only.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%Xb	x-avc-behavior	The web application behavior identified by the AVC engine.
%XB	x-avg-bw	Average bandwidth of the user if bandwidth limits are defined by the AVC engine.
%XC	x-webcat-code-abbr	URL category abbreviation for the URL category assigned to the transaction.
%Xd	x-mcafee-scanverdict	McAfee specific identifier: (scan verdict)
%Xe	x-mcafee-filename	McAfee specific identifier: (File name yielding verdict) This field is written with double-quotes in the access logs.
%Xf	x-mcafee-av-scanerror	McAfee specific identifier: (scan error)
%XF	x-webcat-code-full	Full name of the URL category assigned to the transaction. This field is written with double-quotes in the access logs.
%Xg	x-mcafee-av-detecttype	McAfee specific identifier: (detect type)
%XG	x-avc-reqhead-scanverdict	AVC request header verdict
%Xh	x-mcafee-av-virustype	McAfee specific identifier: (virus type)
%XH	x-avc-reqbody-scanverdict	AVC request body verdict
%Xi	x-webroot-trace-id	Webroot specific scan identifier: (Trace ID)
%Xj	x-mcafee-virus-name	McAfee specific identifier: (virus name). This field is written with double-quotes in the access logs.
%Xk	x-wbrs-threat-type	Web reputation threat type.
%XK	x-wbrs-threat-reason	Web reputation threat reason.
%Xl	x-ids-verdict	Cisco Data Security Policy scanning verdict. If this field is included, it will display the IDS verdict, or "0" if IDS was active but the document scanned clean, or "-" if no IDS policy was active for the request.
%XL	x-webcat-resp-code-full	The URL category verdict determined during response-side scanning, full name. Applies to the Cisco Web Usage Controls URL filtering engine only.
%XM	x-avc-resphead-scanverdict	AVC response header verdict
%Xn	x-webroot-threat-name	Webroot specific identifier: (Threat name) This field is written with double-quotes in the access logs.
%XN	x-avc-reqbody-scanverdict	AVC response body verdict
%XO	x-avc-app	The web application identified by the AVC engine.
%Xp	x-icap-verdict	External DLP server scanning verdict

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%XP	x-acl-added-headers	Unrecognized header. Use this field to log extra headers in client requests. This supports troubleshooting of specialized systems that add headers to client requests as a way of authenticating and redirecting those requests, for example, YouTube for Schools.
%XQ	x-webcat-req-code-abbr	The URL category verdict determined during request-side scanning, abbreviated.
%Xr	x-result-code	Scanning verdict information.
%XR	x-webcat-req-code-full	The URL category verdict determined during request-side scanning, full name.
%Xs	x-webroot-spyid	Webroot specific identifier: (Spy ID)
%XS	x-request-rewrite	Safe browsing scanning verdict. Indicates whether or not either the safe search or site content ratings feature was applied to the transaction.
%Xt	x-webroot-trr	Webroot specific identifier: (Threat Risk Ratio (TRR))
%XT	x-bw-throttled	Flag that indicates whether or not bandwidth limits were applied to the transaction.
%Xu	x-avc-type	The web application type identified by the AVC engine.
%Xv	x-webroot-scanverdict	Malware scanning verdict from Webroot
%XV	x-request-source-ip	The downstream IP address when the “Enable Identification of Client IP Addresses using X-Forwarded-For” check box is enabled for the Web Proxy settings.
%XW	x-wbrs-score	Decoded WBRs score <-10.0-10.0>
%Xx	x-sophos-scanerror	Sophos specific identifier: (scan return code)
%Xy	x-sophos-file-name	The file location where Sophos found the objectionable content. For non-archive files, this value is the file name itself. For archive file, it is the object in the archive, such as <code>archive.zip/virus.exe</code> .
%XY	x-sophos-scanverdict	Sophos specific identifier: (scan verdict)
%Xz	x-sophos-virus-name	Sophos specific identifier: (threat name)
%XZ	x-resp-dvs-verdictname	Unified response-side anti-malware scanning verdict that provides the <i>malware category</i> independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning. This field is written with double-quotes in the access logs.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%X#1#	x-amp-verdict	Verdict from Advanced Malware Protection file scanning: <ul style="list-style-type: none"> “0” indicates the file is clean. “1” indicates the file was not scanned due to its file type. “2” or greater indicates the file is not clean.
%X#2#	x-amp-malware-name	Threat name, as determined by Advanced Malware Protection file scanning. "-" indicates no threat.
%X#3#	x-amp-score	Reputation score from Advanced Malware Protection file scanning. This score is used only if the cloud reputation service is unable to determine a clear verdict for the file. For details, see information about the Threat Score and the reputation threshold in Chapter 16, “File Reputation Filtering and File Analysis.”
%X#4#	x-amp-upload	Indicator of upload and analysis request: “0” indicates that Advanced Malware Protection did not request upload of the file for analysis. “1” indicates that Advanced Malware Protection did request upload of the file for analysis.
%X#5#	x-amp-filename	The name of the file being downloaded and analyzed.
%X#6#	x-amp-sha	The SHA-256 identifier for this file.
%y	cs-method	Method
%Y	cs-url	The entire URL
N/A	x-hierarchy-origin	Code that describes which server was contacted for the retrieving the request content. (e.g. DIRECT/www.example.com)
N/A	x-resultcode-httpstatus	Result code and the HTTP response code, with a slash (/) in between.

Related Topics

- [Interpreting Access Log File Entries, page 20-12.](#)
- [Interpreting W3C Access Logs, page 20-15.](#)

Transaction Result Codes

Transaction result codes in the access log file describe how the appliance resolves client requests. For example, if a request for an object can be resolved from the cache, the result code is `TCP_HIT`. However, if the object is not in the cache and the appliance pulls the object from an origin server, the result code is `TCP_MISS`. The following table describes transaction result codes.

Result Code	Description
<code>TCP_HIT</code>	The object requested was fetched from the disk cache.
<code>TCP_IMS_HIT</code>	The client sent an IMS (If-Modified-Since) request for an object and the object was found in the cache. The proxy responds with a 304 response.
<code>TCP_MEM_HIT</code>	The object requested was fetched from the memory cache.
<code>TCP_MISS</code>	The object was not found in the cache, so it was fetched from the origin server.
<code>TCP_REFRESH_HIT</code>	The object was in the cache, but had expired. The proxy sent an IMS (If-Modified-Since) request to the origin server, and the server confirmed that the object has not been modified. Therefore, the appliance fetched the object from either the disk or memory cache.
<code>TCP_CLIENT_REFRESH_MISS</code>	The client sent a “don’t fetch response from cache” request by issuing the ‘Pragma: no-cache’ header. Due to this header from the client, the appliance fetched the object from the origin server.
<code>TCP_DENIED</code>	The client request was denied due to Access Policies.
<code>UDP_MISS</code>	The object was fetched from the origin server.
<code>NONE</code>	There was an error in the transaction. For example, a DNS failure or gateway timeout.

Related Topics

- [Interpreting Access Log File Entries, page 20-12.](#)
- [Interpreting W3C Access Logs, page 20-15](#)

ACL Decision Tags

An ACL decision tag is a field in an access log entry that indicates how the Web Proxy handled the transaction. It includes information from the Web Reputation filters, URL categories, and the scanning engines.



Note

The end of the ACL decision tag includes a dynamically generated number that the Web Proxy uses internally to increase performance. You can ignore this number.

The following table describes the ACL decision tag values.

ACL Decision Tag	Description
ALLOW_ADMIN_ERROR_PAGE	The Web Proxy allowed the transaction to an notification page and to any logo used on that page.
ALLOW_CUSTOMCAT	The Web Proxy allowed the transaction based on custom URL category filtering settings for the Access Policy group.
ALLOW_WBRS	The Web Proxy allowed the transaction based on the Web Reputation filter settings for the Access Policy group.
BLOCK_ADMIN	The Web Proxy blocked the transaction based on some default settings for the Access Policy group.
BLOCK_ADMIN_CONNECT	The Web Proxy blocked the transaction based on the TCP port of the destination as defined in the HTTP CONNECT Ports setting for the Access Policy group.
BLOCK_ADMIN_CUSTOM_USER_AGENT	The Web Proxy blocked the transaction based on the user agent as defined in the Block Custom User Agents setting for the Access Policy group.
BLOCK_ADMIN_IDS	The Web Proxy blocked the transaction based on the MIME type of the request body content as defined in the Data Security Policy group.
BLOCK_ADMIN_FILE_TYPE	The Web Proxy blocked the transaction based on the file type as defined in the Access Policy group.
BLOCK_ADMIN_PROTOCOL	The Web Proxy blocked the transaction based on the protocol as defined in the Block Protocols setting for the Access Policy group.
BLOCK_ADMIN_SIZE	The Web Proxy blocked the transaction based on the size of the response as defined in the Object Size settings for the Access Policy group.
BLOCK_ADMIN_SIZE_IDS	The Web Proxy blocked the transaction based on the size of the request body content as defined in the Data Security Policy group.
BLOCK_AMP_RESP	The Web Proxy blocked the response based on the Advanced Malware Protection settings for the Access Policy group.
BLOCK_AMW_REQ	The Web Proxy blocked the request based on the Anti-Malware settings for the Outbound Malware Scanning Policy group. The request body produced a positive malware verdict.
BLOCK_AMW_RESP	The Web Proxy blocked the response based on the Anti-Malware settings for the Access Policy group.
BLOCK_AMW_REQ_URL	The Web Proxy suspects the URL in the HTTP request might not be safe, so it blocked the transaction at request time based on the Anti-Malware settings for the Access Policy group.
BLOCK_AVC	The Web Proxy blocked the transaction based on the configured Application settings for the Access Policy group.

ACL Decision Tag	Description
BLOCK_CONTENT_UNSAFE	The Web Proxy blocked the transaction based on the site content ratings settings for the Access Policy group. The client request was for adult content and the policy is configured to block adult content.
BLOCK_CONTINUE_CONTENT_UNSAFE	The Web Proxy blocked the transaction and displayed the Warn and Continue page based on the site content ratings settings in the Access Policy group. The client request was for adult content and the policy is configured to give a warning to users accessing adult content.
BLOCK_CONTINUE_CUSTOMCAT	The Web Proxy blocked the transaction and displayed the Warn and Continue page based on a custom URL category in the Access Policy group configured to “Warn.”
BLOCK_CONTINUE_WEBCAT	The Web Proxy blocked the transaction and displayed the Warn and Continue page based on a predefined URL category in the Access Policy group configured to “Warn.”
BLOCK_CUSTOMCAT	The Web Proxy blocked the transaction based on custom URL category filtering settings for the Access Policy group.
BLOCK_ICAP	The Web Proxy blocked the request based on the verdict of the external DLP system as defined in the External DLP Policy group.
BLOCK_SEARCH_UNSAFE	The client request included an unsafe search query and the Access Policy is configured to enforce safe searches, so the original client request was blocked.
BLOCK_SUSPECT_USER_AGENT	The Web Proxy blocked the transaction based on the Suspect User Agent setting for the Access Policy group.
BLOCK_UNSUPPORTED_SEARCH_APP	The Web Proxy blocked the transaction based on the safe search settings for the Access Policy group. The transaction was for an unsupported search engine, and the policy is configured to block unsupported search engines.
BLOCK_WBRS	The Web Proxy blocked the transaction based on the Web Reputation filter settings for the Access Policy group.
BLOCK_WBRS_IDS	The Web Proxy blocked the upload request based on the Web Reputation filter settings for the Data Security Policy group.
BLOCK_WEBCAT	The Web Proxy blocked the transaction based on URL category filtering settings for the Access Policy group.
BLOCK_WEBCAT_IDS	The Web Proxy blocked the upload request based on the URL category filtering settings for the Data Security Policy group.
DECRYPT_ADMIN	The Web Proxy decrypted the transaction based on some default settings for the Decryption Policy group.
DECRYPT_WEBCAT	The Web Proxy decrypted the transaction based on URL category filtering settings for the Decryption Policy group.
DECRYPT_WBRS	The Web Proxy decrypted the transaction based on the Web Reputation filter settings for the Decryption Policy group.

ACL Decision Tag	Description
DEFAULT_CASE	The Web Proxy allowed the client to access the server because none of the AsyncOS services, such as Web Reputation or anti-malware scanning, took any action on the transaction.
DROP_ADMIN	The Web Proxy dropped the transaction based on some default settings for the Decryption Policy group.
DROP_WEBCAT	The Web Proxy dropped the transaction based on URL category filtering settings for the Decryption Policy group.
DROP_WBRS	The Web Proxy dropped the transaction based on the Web Reputation filter settings for the Decryption Policy group.
MONITOR_AMP_RESP	The Web Proxy monitored the server response based on the Advanced Malware Protection settings for the Access Policy group.
MONITOR_AMW_RESP	The Web Proxy monitored the server response based on the Anti-Malware settings for the Access Policy group.
MONITOR_AMW_RESP_URL	The Web Proxy suspects the URL in the HTTP request might not be safe, but it monitored the transaction based on the Anti-Malware settings for the Access Policy group.
MONITOR_AVC	The Web Proxy monitored the transaction based on the Application settings for the Access Policy group.
MONITOR_CONTINUE_CONTENT_UNSAFE	Originally, the Web Proxy blocked the transaction and displayed the Warn and Continue page based on the site content ratings settings in the Access Policy group. The client request was for adult content and the policy is configured to give a warning to users accessing adult content. The user accepted the warning and continued to the originally requested site, and no other scanning engine subsequently blocked the request.
MONITOR_CONTINUE_CUSTOMCAT	Originally, the Web Proxy blocked the transaction and displayed the Warn and Continue page based on a custom URL category in the Access Policy group configured to "Warn." The user accepted the warning and continued to the originally requested site, and no other scanning engine subsequently blocked the request.
MONITOR_CONTINUE_WEBCAT	Originally, the Web Proxy blocked the transaction and displayed the Warn and Continue page based on a predefined URL category in the Access Policy group configured to "Warn." The user accepted the warning and continued to the originally requested site, and no other scanning engine subsequently blocked the request.
MONITOR_IDS	The Web Proxy scanned the upload request using either a Data Security Policy or an External DLP Policy, but did not block the request. It evaluated the request against the Access Policies.
MONITOR_SUSPECT_USER_AGENT	The Web Proxy monitored the transaction based on the Suspect User Agent setting for the Access Policy group.

ACL Decision Tag	Description
MONITOR_WBRS	The Web Proxy monitored the transaction based on the Web Reputation filter settings for the Access Policy group.
NO_AUTHORIZATION	The Web Proxy did not allow the user access to the application because the user was already authenticated against an authentication realm, but not against any authentication realm configured in the Application Authentication Policy.
NO_PASSWORD	The user failed authentication.
PASSTHRU_ADMIN	The Web Proxy passed through the transaction based on some default settings for the Decryption Policy group.
PASSTHRU_WEBCAT	The Web Proxy passed through the transaction based on URL category filtering settings for the Decryption Policy group.
PASSTHRU_WBRS	The Web Proxy passed through the transaction based on the Web Reputation filter settings for the Decryption Policy group.
REDIRECT_CUSTOMCAT	The Web Proxy redirected the transaction to a different URL based on a custom URL category in the Access Policy group configured to “Redirect.”
SAAS_AUTH	The Web Proxy allowed the user access to the application because the user was authenticated transparently against the authentication realm configured in the Application Authentication Policy.
OTHER	The Web Proxy did not complete the request due to an error, such as an authorization failure, server disconnect, or an abort from the client.

Related Topics

- [Interpreting Access Log File Entries, page 20-12.](#)
- [Interpreting W3C Access Logs, page 20-15.](#)

Malware Scanning Verdict Values

A malware scanning verdict is a value assigned to a URL request or server response that determines the probability that it contains malware. The Webroot, McAfee, and Sophos scanning engines return the malware scanning verdict to the DVS engine so the DVS engine can determine whether to monitor or block the scanned object. Each malware scanning verdict corresponds to a malware category listed on the Access Policies > Reputation and Anti-Malware Settings page when you edit the anti-malware settings for a particular Access Policy.

The following lists the different Malware Scanning Verdict Values and each malware category with which they correspond:

Malware Scanning Verdict Value	Malware Category
-	Not Set
0	Unknown

Malware Scanning Verdict Value	Malware Category
1	Not Scanned
2	Timeout
3	Error
4	Unscannable
10	Generic Spyware
12	Browser Helper Object
13	Adware
14	System Monitor
18	Commercial System Monitor
19	Dialer
20	Hijacker
21	Phishing URL
22	Trojan Downloader
23	Trojan Horse
24	Trojan Phisher
25	Worm
26	Encrypted File
27	Virus
33	Other Malware
34	PUA
35	Aborted
36	Outbreak Heuristics
37	Known Malicious and High-Risk Files

Related Topics

- [Interpreting Access Log File Entries, page 20-12.](#)
- [Interpreting W3C Access Logs, page 20-15.](#)

Troubleshooting Logging

- [Custom URL Categories Not Appearing in Access Log Entries, page A-6](#)
- [Logging HTTPS Transactions, page A-6](#)
- [Alert: Unable to Maintain the Rate of Data Being Generated, page A-7](#)
- [Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs, page A-7](#)



Perform System Administration Tasks

- [Overview of System Administration, page 21-1](#)
- [Saving and Loading the Appliance Configuration, page 21-2](#)
- [Support Commands, page 21-3](#)
- [Working with Feature Keys, page 21-6](#)
- [Administering User Accounts, page 21-7](#)
- [Defining User Preferences, page 21-11](#)
- [Configuring Administrator Settings, page 21-12](#)
- [Configuring the Return Address for Generated Messages, page 21-13](#)
- [Managing Alerts, page 21-13](#)
- [FIPS Compliance, page 21-20](#)
- [System Date and Time Management, page 21-22](#)
- [Installing a Server Digital Certificate, page 21-23](#)
- [AsyncOS for Web Upgrades and Updates, page 21-26](#)
- [Reverting to a Previous Version of AsyncOS for Web, page 21-32](#)

Overview of System Administration

The S-Series appliance provides a variety of tools for managing the system. Functionality on System Administration tab helps you manage the following tasks:

- Appliance configuration
- Feature keys
- Adding, editing, and removing user accounts
- AsyncOS software upgrades and updates
- System time

Saving and Loading the Appliance Configuration

All configuration settings within the Web Security appliance are managed using a single XML configuration file.

Viewing and Printing the Appliance Configuration

-
- Step 1** Choose **System Administration > Configuration Summary**.
- Step 2** View or print the Configuration Summary page as required.
-

Saving the Appliance Configuration File

-
- Step 1** Choose **System Administration > Configuration File**.
- Step 2** Complete the Configuration File options.

Option	Description
Choose from these location options: <ul style="list-style-type: none"> Download file to local computer to view or save Save file to this appliance (example.com) Email file to 	Allows you to choose where to save the file to
Mask passwords in the Configuration Files	If enabled, causes the original, encrypted password to be replaced with “*****” in the exported or saved file. Please note, however, that configuration files with masked passwords cannot be loaded directly back into AsyncOS for Web.
Choose from these file name options: <ul style="list-style-type: none"> Use system-generated file name Use user-defined file name: 	Allows you to choose the configuration file naming method.

- Step 3** Click **Submit**.
-

Loading the Appliance Configuration File



Warning

Loading configuration will permanently remove all of your current configuration settings. It is strongly recommended that you save your configuration before performing these actions.

-
- Step 1** Choose **System Administration > Configuration File**.
- Step 2** Choose a Load Configuration option and a file to load. Note:
- Files with masked passwords cannot be loaded.
 - Files must have the following header:


```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE config SYSTEM "config.dtd">
```

 and a correctly formatted config section:


```
<config> ... your configuration information in valid XML </config>
```
- Step 3** Click **Load**.
- Step 4** Read the warning displayed. If you understand the consequences of proceeding, click **Continue**.
-



Note If a compatible configuration file is based on an older version of the set of URL categories than the version currently installed on the appliance, policies and identities in the configuration file may be modified automatically.

Support Commands

Opening a Technical Support Request

You can use the appliance to send a non-urgent request for assistance to Cisco Customer Support. When the appliance sends the request, it also sends the configuration of the appliance. The appliance must be able to send mail to the Internet to send a support request.



Note If you have an urgent issue, please call a Cisco Worldwide Support Center.

Before You Begin

- Verify that your Cisco.com user ID is associated with your service agreement contract for this appliance. To view a list of service contracts that are currently associated with your Cisco.com profile, visit the Cisco.com Profile Manager at <https://sso.cisco.com/autho/forms/CDClogin.html>. If you do not have a Cisco.com user ID, register to get one.
-

- Step 1** Choose **Support And Help > Contact Technical Support**.
- Step 2** (Optional) Choose additional recipients for the request. By default, the support request and configuration file is sent to Cisco Customer Support.
- Step 3** Enter your contact information.
- Step 4** Enter the issue details.
- If you have a customer support ticket already for this issue, enter it.
- Step 5** Click **Send**. A trouble ticket is created with Cisco.
-

Enabling Remote Access to the Web Security appliance

The Remote Access option allows Cisco Customer Support to remotely access your Web Security appliance for support purposes.

-
- Step 1** Choose **Support And Help > Remote Access**.
- Step 2** Click **Enable**.
- Step 3** Complete the Customer Support Remote Access options:

Option	Description
Customer Support Password	A password that you will provide to your Cisco Customer Support representative, along with the appliance system serial number (physical appliance) or VLN (virtual appliance). The customer support representative will use these details to generate a password to access your appliance. Customer support will not directly use the password entered here to access the system.
Secure Tunnel (recommended)	<p>Specifies whether or not to use a secure tunnel for remote access connections.</p> <p>When enabled, the appliance creates an SSH tunnel over the specified port to the server <code>upgrades.ironport.com</code>, over port 443 (by default). Once a connection is made, Cisco Customer Support is able to use the SSH tunnel to obtain access to the appliance.</p> <p>Once the techsupport tunnel is enabled, it will remain connected to <code>upgrades.ironport.com</code> for 7 days. After 7 days, no new connections can be made using the techsupport tunnel, though any existing connections will continue to exist and work.</p> <p>The Remote Access account will remain active until specifically deactivated.</p>

- Step 4** Submit and commit your changes.
-

Packet Capture

The appliance provides the ability to capture and display TCP/IP and other packets being transmitted or received over the network to which the appliance is attached.



Note

The packet capture feature is similar to the Unix `tcpdump` command.

Starting a Packet Capture

-
- Step 1** Choose **Support and Help > Packet Capture**.

Step 2 (Optional) Click **Edit Settings** to change the packet capture settings.

Option	Description
Capture File Size Limit	Specifies the maximum size that the capture file can reach. Once the limit is reached, the data will be discarded and a new file started, unless the Capture Duration setting is 'Run Capture Until File Size Limit Reached.'
Capture Duration	Options for if and when the capture automatically stops. Choose from: <ul style="list-style-type: none"> • Run Capture Until File Size Limit Reached. The capture runs until the file limit set above is reached. • Run Capture Until Time Elapsed Reaches. The capture runs for a specified duration. If you enter the amount of time without specifying the units, AsyncOS uses seconds by default. • Run Capture Indefinitely. The packet capture runs until you manually stop it. <p>Note The capture can be ended manually at any time.</p>
Interfaces	The interfaces from which traffic will be captured.
Filters	The filtering options to apply when capturing packets. Filtering allows you to capture required packets only. Choose from: <ul style="list-style-type: none"> • No Filters. All packets will be captured. • Predefined Filters. The predefined filters provide filtering by port and/or IP addresses. If left blank, all traffic will be captured. • Custom Filter. Use this option if you already know the exact syntax of the packet capture options that you need. Use standard tcpdump syntax.

(Optional) Submit and commit your packet capture changes.



Note When you change the packet capture settings without committing the changes and then start a packet capture, AsyncOS uses the new settings. This allows you to use the new settings in the current session without enforcing the settings for future packet capture runs. The settings remain in effect until you clear them.

Step 3 Click **Start Capture**. To manually stop a running capture, click **Stop Capture**.

Managing Packet Capture Files

The appliance saves the captured packet activity to a file and stores the file locally. You can send packet capture files using FTP to Cisco Customer Support for debugging and troubleshooting purposes.

Downloading or Deleting Packet Capture Files

Step 1 Choose **Support and Help > Packet Capture**.

Step 2 Select the packet capture file you wish to use from the Manage Packet Capture Files pane. If this pane is not visible then no packet capture files have been stored on the appliance.

Step 3 Click **Download File** or **Delete Selected Files** as required.

**Note**

You can also connect to the appliance using FTP and retrieving packet capture files from the captures directory.

Working with Feature Keys

Feature keys enable specific functionality on your system. Keys are specific to the serial number of your appliance (you cannot re-use a key from one system on another system).

**Note**

Feature keys for the Web Security Virtual appliance are included in the virtual appliance license file and cannot be installed separately.

Displaying and Updating Feature Keys

Step 1 Choose **System Administration > Feature Keys**.

Step 2 To refresh the list of pending keys, click **Check for New Keys** to refresh the list of pending keys.

Step 3 To add a new feature key manually, paste or type the key into the Feature Key field and click **Submit Key**. If the feature key is valid, the feature key is added to the display.

Step 4 To activate a new feature key from the Pending Activation list, mark its “Select” checkbox and click **Activate Selected Keys**.

You can configure your appliance to automatically download and install new keys as they are issued. In this case, the Pending Activation list will always be empty. You can tell AsyncOS to look for new keys at any time by clicking the **Check for New Keys** button, even if you have disabled the automatic checking via the Feature Key Settings page.

Changing Feature Key Update Settings

The Feature Key Settings page is used to control whether your appliance checks for and downloads new feature keys, and whether or not those keys are automatically activated.

Step 1 Choose **System Administration > Feature Key Settings**.

Step 2 Click **Edit Settings**.

Step 3 Change the Feature Key Settings as required.

Option	Description
Automatic Serving of Feature Keys	Options to automatically check and download feature keys and to automatically activate downloaded feature keys. Automatic checks are normally performed once a month but this changes to once a day when a feature key is to expire in less than 10 days and once a day after key expiration, for up to one month. After a month, the expired key is no longer included in the list of expiring/expired keys.

Step 4 Submit and commit your changes.

Virtual Appliance License

The Cisco Web Security Virtual appliance requires an additional license to run the virtual appliance on a host. You can use this license for multiple, cloned virtual appliances.

Feature keys are included as part of the virtual appliance license. The feature keys expire at the same time as the license, even if the key has not been activated yet. Purchasing new feature keys will require downloading and installing a new virtual appliance license.

Due to feature keys being included in the virtual appliance license, there are no 30-day evaluations for AsyncOS for Web features.



Note

You cannot open a Technical Support tunnel before installing the virtual appliance license.

Installing a Virtual Appliance License

Before You Begin

- (Optional) See the *Cisco Security Virtual Appliance Installation Guide* for more detailed information about installing a virtual appliance license.

Step 1 Run the `loadlicense` CLI command.

Step 2 Copy and paste the license into the CLI.

Administering User Accounts

The following types of users can log into the Web Security appliance to manage the appliance:

- **Local users.** You can define users locally on the appliance itself.
- **Users defined in an external system.** You can configure the appliance to connect to an external RADIUS server to authenticate users logging into the appliance.

**Note**

Any user you define can log into the appliance using any method, such as logging into the web interface or using SSH.

Related Topics

- [Managing Local User Accounts, page 21-8.](#)
- [RADIUS User Authentication, page 21-10.](#)

Managing Local User Accounts

You can define any number of users locally on the Web Security appliance.

The default system admin account has all administrative privileges. You can change the admin account password, but you cannot edit or delete this account.

**Note**

If you have lost the admin user password, contact your Cisco support provider.

Adding Local User Accounts

-
- Step 1** Choose **System Administration > Users**.
- Step 2** Click **Add User**
- Step 3** Enter a username, noting the following rules:
- Usernames can contain lowercase letters, numbers, and the dash (-) character, but cannot begin with a dash.
 - Usernames cannot greater than 16 characters.
 - Usernames cannot be special names that are reserved by the system, such as “operator” or “root.”
 - If you also use external authentication, usernames should not duplicate externally-authenticated usernames.
- Step 4** Enter a full name for the user.
- Step 5** Select a user type.

User Type	Description
Administrator	Allows full access to all system configuration settings. However, the <code>upgradecheck</code> and <code>upgradeinstall</code> CLI commands can be issued only from the system defined “admin” account.
Operator	Restricts users from creating, editing, or removing user accounts. The operators group also restricts the use of the following CLI commands: <ul style="list-style-type: none"> • <code>resetconfig</code> • <code>upgradecheck</code> • <code>upgradeinstall</code> • <code>systemsetup</code> or running the System Setup Wizard

User Type	Description
Read-Only Operator	User accounts with this role: <ul style="list-style-type: none"> • Can view configuration information. • Can make and submit changes to see how to configure a feature, but they cannot commit them. • Cannot make any other changes to the appliance, such as clearing the cache or saving files. • Cannot access the file system, FTP, or SCP.
Guest	The guests group users can only view system status information, including reporting and tracking.

Step 6 Enter a password of at least 6 characters and retype it.

Step 7 Submit and commit your changes.

Deleting User Accounts

Step 1 Choose **System Administration > Users**.

Step 2 Click the trash can icon corresponding to the listed user name and confirm when prompted.

Step 3 Submit and commit your changes.

Editing User Accounts

Step 1 Choose **System Administration > Users**.

Step 2 Click the user name.

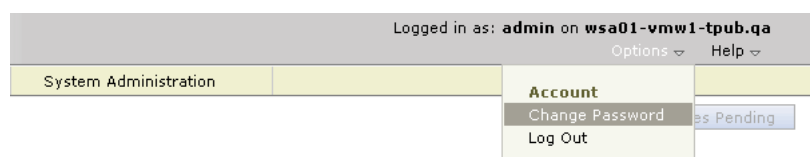
Step 3 Make changes to the user on the Edit User page as required.

Step 4 Submit and commit your changes.

Changing Passwords

To change the password of the account currently logged in, use the **Options > Change Password** option located on the top right-hand side of the web interface, as shown:

Figure 21-1 The Change Password Option



For other accounts, edit the account and change the password in the Local User Settings page.

Related Topics

- [Editing User Accounts, page 21-9](#)

RADIUS User Authentication

The Web Security appliance can use a RADIUS directory service to authenticate users that log in to the appliance using HTTP, HTTPS, SSH, and FTP. You can configure the appliance to contact multiple external servers for authentication, using either PAP or CHAP authentication. You can map external users accounts to different Web Security appliance user role types.

Sequence of Events For Radius Authentication

When external authentication is enabled and a user logs into the Web Security appliance, the appliance:

1. determines if the user is the system defined “admin” account.
2. If not, checks the first configured external server to determine if the user is defined there.
3. If the appliance cannot connect to the first external server, it checks the next external server in the list.
4. If the appliance cannot connect to any external server, it tries to authenticate the user as a local user defined on the Web Security appliance.
5. If the user does not exist on any external server or on the appliance, or if the user enters the wrong password, access to the appliance is denied.

Enabling External Authentication Using RADIUS

-
- Step 1** On the System Administration > Users page, click **Enable**.
- Step 2** Check the **Enable External Authentication** checkbox.
- Step 3** Enter the hostname, port number, and Shared Secret password for the RADIUS server.
- Step 4** Enter the number of seconds for the appliance to wait for a response from the server before timing out.
- Step 5** Choose the authentication protocol used by the RADIUS server.
- Step 6** (Optional) Click **Add Row** to add another RADIUS server. Repeat steps 3–5 for each RADIUS server.



Note You can add up to ten RADIUS servers.

- Step 7** Enter the number of seconds AsyncOS stores the external authentication credentials before contacting the RADIUS server again to re-authenticate in the “External Authentication Cache Timeout” field. Default is zero (0).



Note If the RADIUS server uses one-time passwords, for example passwords created from a token, enter zero (0). When the value is set to zero, AsyncOS does not contact the RADIUS server again to authenticate during the current session.

Step 8 Configure Group Mapping:

Setting	Description
Map externally authenticated users to multiple local roles.	<p>AsyncOS assigns RADIUS users to appliance roles based on the RADIUS CLASS attribute. CLASS attribute requirements:</p> <ul style="list-style-type: none"> • 3 character minimum • 253 character maximum • no colons, commas, or newline characters • one or more mapped CLASS attributes for each RADIUS user (With this setting, AsyncOS denies access to RADIUS users without a mapped CLASS attribute.) <p>For RADIUS users with multiple CLASS attributes, AsyncOS assigns the most restrictive role. For example, if a RADIUS user has two CLASS attributes, which are mapped to the Operator and Read-Only Operator roles, AsyncOS assigns the RADIUS user to the Read-Only Operator role, which is more restrictive than the Operator role.</p> <p>These are the appliance roles ordered from least restrictive to most restrictive:</p> <ul style="list-style-type: none"> • Administrator • Operator • Read-Only Operator • Guest
Map all externally authenticated users to the Administrator role.	AsyncOS assigns RADIUS users to the Administrator role.

Step 9 Choose whether to map all externally authenticated users to the Administrator role or to different appliance user role types.

Step 10 If you map users to different role types, enter the group name as defined in the RADIUS CLASS attribute in the Group Name or Directory field, and choose an appliance role type from the Role field. You can add more role mappings by clicking **Add Row**.

Step 11 Submit and commit your changes.

Related Topics

- For more information on user role types, see [Adding Local User Accounts, page 21-8](#).

Defining User Preferences

Preference settings, such as reporting display formats, are stored for each user and are the same regardless from which client machine the user logs into the appliance.

Step 1 Choose **Options > Preferences**.

Step 2 On the User Preferences page, click **Edit Preferences**.

Step 3 Configure the preference settings as required.

Preference Setting	Description
Language Display	The language AsyncOS for Web uses in the web interface and CLI.
Landing Page	The page that displays when the user logs into the appliance.
Reporting Time Range Displayed (default)	The default time range that displays for reports on the Reporting tab.
Number of Reporting Rows Displayed	The number of rows of data shown for each report by default.

Step 4 Submit and commit your changes.

Configuring Administrator Settings

You can configure the Web Security appliance to have stricter access requirements for administrators logging into the appliance.

Command	Description
adminaccessconfig > banner	Configures the appliance to display any text you specify when an administrator tries to logs in. The custom banner text appears when an administrator tries to access the appliance through all interfaces, such as the web interface or via FTP. You can load the custom text by either pasting it into the CLI prompt or by copying it from a file located on the Web Security appliance. To upload the text from a file, you must first transfer the file to the configuration directory on the appliance using FTP
adminaccessconfig > ipaccess	Controls from which IP addresses administrators access the Web Security appliance. Administrators can access the appliance from any machine or from machines with an IP address from a list you specify. When restrict access to an allow list, you can specify IP addresses, subnets, or CIDR addresses. By default, when you list the addresses that can access the appliance, the IP address of your current machine is listed as the first address in the allow list. You cannot delete the IP address of your current machine from the allow list.
adminaccessconfig > strictssl	Configures the appliance so administrators log into the web interface on port 8443 using stronger SSL ciphers (greater than 56 bit encryption). When you configure the appliance to require stronger SSL ciphers, the change only applies to administrators accessing the appliance using HTTPS to manage the appliance. It does not apply to other network traffic connected to the Web Proxy using HTTPS.

Configuring the Return Address for Generated Messages

You can configure the return address for mail generated by AsyncOS for reports.

-
- Step 1** Choose **System Administration > Return Addresses**.
 - Step 2** Click **Edit Settings**.
 - Step 3** Enter the display name, user name, and domain name.
 - Step 4** Submit and commit your changes.
-

Managing Alerts

Alerts are email notifications containing information about events occurring on the Cisco Web Security Appliance appliance. These events can be of varying levels of importance (or severity) from minor (Informational) to major (Critical) and pertain generally to a specific component or feature on the appliance.

**Note**

To receive alerts and email notifications, you must configure the SMTP relay host that the appliance uses to send the email messages.

Alert Classifications and Severities

The information contained in an alert is determined by an alert classification and a severity. You can specify which alert classifications, at which severity, are sent to any alert recipient.

Alert Classifications

AsyncOS sends the following types of alert:

- System
- Hardware
- Updater
- Web Proxy
- Anti-Malware
- L4 Traffic Monitor

Alert Severities

Alerts can be sent for the following severities:

- **Critical:** Requires immediate attention.
- **Warning:** Problem or error requiring further monitoring and potentially immediate attention.
- **Information:** Information generated in the routine functioning of this device.

Managing Alert Recipients

**Note**

If you enabled AutoSupport during System Setup, the email address you specified will receive alerts for all severities and classes by default. You can change this configuration at any time.

Adding and Editing Alert Recipients

-
- Step 1** Choose **System Administration > Alerts**.
 - Step 2** Click on a recipient in the Alert Recipients list to edit it, or click **Add Recipient** to add a new recipient.
 - Step 3** Add or edit the recipient's email address. You can enter multiple addresses, separated by commas.
 - Step 4** Select which alert severities to receive for each alert type.
 - Step 5** Submit and commit your changes.
-

Deleting Alert Recipients

-
- Step 1** Choose **System Administration > Alerts**.
 - Step 2** Click the trash can icon corresponding to the alert recipient in the Alert Recipient listing and confirm.
 - Step 3** Commit your changes.
-

Configuring Alert Settings

Alert settings are global settings, meaning that they affect how all of the alerts behave.

-
- Step 1** Choose **System Administration > Alerts**.
 - Step 2** Click **Edit Settings**.

Step 3 Configure the alert settings as required.

Option	Description
From Address to Use When Sending Alerts	The RFC 2822 compliant “Header From:” address to use when sending alerts. An option is provided to automatically generate an address based on the system hostname (“alert@<hostname>”)
Wait Before Sending a Duplicate Alert	Specifies the time interval for duplicate alerts. There are two settings: Initial Number of Seconds to Wait Before Sending a Duplicate Alert. If you set this value to 0, duplicate alert summaries are not sent and instead, all duplicate alerts are sent without any delay (this can lead to a large amount of email over a short amount of time). The number of seconds to wait between sending duplicate alerts (alert interval) is increased after each alert is sent. The increase is the number of seconds to wait plus twice the last interval. So a 5 second wait would have alerts sent at 5 seconds, 15, seconds, 35 seconds, 75 seconds, 155 seconds, 315 seconds, etc. Maximum Number of Seconds to Wait Before Sending a Duplicate Alert. You can set a cap on the number of seconds to wait between intervals via the maximum number of seconds to wait before sending a duplicate alert field. For example, if you set the initial value to 5 seconds, and the maximum value to 60 seconds, alerts would be sent at 5 seconds, 15 seconds, 35 seconds, 60 seconds, 120 seconds, etc
Cisco AutoSupport	Specifies whether or not to send Cisco the following support information: <ul style="list-style-type: none"> • a copy of all alert messages generated by the system • weekly reports noting the uptime of the system, the output of the <code>status</code> command, and the AsyncOS version used. Also specifies whether or not to send internal alert recipients a copy of every message sent to Cisco. This applies only to recipients that are set to receive System alerts at Information severity level.

Step 4 Submit and commit your changes.

Alert Listing

The following sections list alerts by classification. The table in each section includes the alert name (internally used descriptor), actual text of the alert, description, severity (critical, information, or warning) and the parameters (if any) included in the text of the message.

Feature Key Alerts

The following table contains a list of the various feature key alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
A "\$feature" key was downloaded from the key server and placed into the pending area. EULA acceptance required.	Information.	\$feature: Name of the feature.
Your "\$feature" evaluation key has expired. Please contact your authorized sales representative.	Warning.	\$feature: Name of the feature.
Your "\$feature" evaluation key will expire in under \$days day(s). Please contact your authorized sales representative.	Warning.	\$feature: Name of the feature. \$days: The number of days that will pass before the feature key will expire.

Hardware Alerts

The following table contains a list of the various hardware alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
A RAID-event has occurred: \$error	Warning	\$error: Text of the RAID error.

Logging Alerts

The following table contains a list of the various logging alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
\$error.	Information.	\$error: The traceback string of the error.
Log Error: Subscription \$name: Log partition is full.	Critical.	\$name: Log subscription name.
Log Error: Push error for subscription \$name: Failed to connect to \$ip: \$reason.	Critical.	\$name: Log subscription name. \$ip: IP address of the remote host. \$reason: Text describing the connect error
Log Error: Push error for subscription \$name: An FTP command failed to \$ip: \$reason.	Critical.	\$name: Log subscription name. \$ip: IP address of the remote host. \$reason: Text describing what went wrong.
Log Error: Push error for subscription \$name: SCP failed to transfer to \$ip:\$port: \$reason',	Critical.	\$name: Log subscription name. \$ip: IP address of the remote host. \$port: Port number on the remote host. \$reason: Text describing what went wrong.

Message	Alert Severity	Parameters
Log Error: 'Subscription \$name: Failed to connect to \$hostname (\$ip): \$error.	Critical.	\$name: Log subscription name. \$hostname: Hostname of the syslog server. \$ip: IP address of the syslog server. \$error: Text of the error message.
Log Error: Subscription \$name: Network error while sending log data to syslog server \$hostname (\$ip): \$error	Critical.	\$name: Log subscription name. \$hostname: Hostname of the syslog server. \$ip: IP address of the syslog server. \$error: Text of the error message.
Subscription \$name: Timed out after \$timeout seconds sending data to syslog server \$hostname (\$ip).	Critical.	\$name: Log subscription name. \$timeout: Timeout in seconds. \$hostname: Hostname of the syslog server. \$ip: IP address of the syslog server.
Subscription \$name: Syslog server \$hostname (\$ip) is not accepting data fast enough.	Critical.	\$name: Log subscription name. \$hostname: Hostname of the syslog server. \$ip: IP address of the syslog server.
Subscription \$name: Oldest log file(s) were removed because log files reached the maximum number of \$max_num_files. Files removed include: \$files_removed.	Information.	\$name: Log subscription name. \$max_num_files: Maximum number of files allowed per log subscription. \$files_removed: List of files that were removed.

Reporting Alerts

The following table contains a list of the various reporting alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.	Critical.	Not applicable.
The reporting system is now able to handle new data.	Information.	Not applicable.
A failure occurred while building periodic report '\$report_title'. This subscription should be examined and deleted if its configuration details are no longer valid.	Critical.	\$report_title: Title of the report.
A failure occurred while emailing periodic report '\$report_title'. This subscription has been removed from the scheduler.	Critical.	\$report_title: Title of the report.

Message	Alert Severity	Parameters
<p>Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above \$threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc).</p> <p>Once disk usage drops below \$threshold percent, full processing of reporting data will be restarted automatically.</p>	Warning.	\$threshold: Threshold value.
<p>PERIODIC REPORTS: While building periodic report \$report_title' the expected domain specification file could not be found at '\$file_name'. No reports were sent.</p>	Critical.	\$report_title: Title of the report. \$file_name: Name of the file.
<p>Counter group "\$counter_group" does not exist.</p>	Critical.	\$counter_group: Name of the counter_group.
<p>PERIODIC REPORTS: While building periodic report \$report_title' the domain specification file '\$file_name' was empty. No reports were sent.</p>	Critical.	\$report_title: Title of the report. \$file_name: Name of the file.
<p>PERIODIC REPORTS: Errors were encountered while processing the domain specification file '\$file_name' for the periodic report '\$report_title'. Any line which has any reported problem had no report sent.</p> <p>\$error_text</p>	Critical.	\$report_title: Title of the report. \$file_name: Name of the file. \$error_text: List of errors encountered.
<p>Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above \$threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc).</p> <p>Once disk usage drops below \$threshold percent, full processing of reporting data will be restarted automatically.</p>	Warning.	\$threshold: Threshold value.
<p>The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled.</p> <p>The error message is:</p> <p>\$err_msg</p>	Critical.	\$err_msg: Error message text.

System Alerts

The following table contains a list of the various system alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
Startup script \$name exited with error: \$message	Critical.	\$name: Name of the script. \$message: Error message text.
System halt failed: \$exit_status: \$output',	Critical.	\$exit_status: Exit code of the command. \$output: Output from the command.
System reboot failed: \$exit_status: \$output	Critical.	\$exit_status: Exit code of the command. \$output: Output from the command.
Process \$name listed \$dependency as a dependency, but it does not exist.	Critical.	\$name: Name of the process. \$dependency: Name of the dependency that was listed.
Process \$name listed \$dependency as a dependency, but \$dependency is not a wait_init process.	Critical.	\$name: Name of the process. \$dependency: Name of the dependency that was listed.
Process \$name listed itself as a dependency.	Critical.	\$name: Name of the process.
Process \$name listed \$dependency as a dependency multiple times.	Critical.	\$name: Name of the process. \$dependency: Name of the dependency that was listed.
Dependency cycle detected: \$cycle.	Critical.	\$cycle: The list of process names involved in the cycle.
An error occurred while attempting to share statistical data through the Network Participation feature. Please forward this tracking information to your support provider: Error: \$error.	Warning.	\$error: The error message associated with the exception.
There is an error with "\$name".	Critical.	\$name: Name of the process that generated a core file.
An application fault occurred: "\$error"	Critical.	\$error: Text of the error, typically a traceback.
Tech support: Service tunnel has been enabled, port \$port	Information.	\$port: Port number used for the service tunnel.

Message	Alert Severity	Parameters
Tech support: Service tunnel has been disabled.	Information.	Not applicable.
<ul style="list-style-type: none"> The host at \$ip has been added to the blacklist because of an SSH DOS attack. The host at \$ip has been permanently added to the ssh whitelist. The host at \$ip has been removed from the blacklist 	Warning.	<p>\$ip - IP address from which a login attempt occurred.</p> <p>Description:</p> <p>IP addresses that try to connect to the appliance over SSH but do not provide valid credentials are added to the SSH blacklist if more than 10 failed attempts occur within two minutes.</p> <p>When a user logs in successfully from the same IP address, that IP address is added to the whitelist.</p> <p>Addresses on the whitelist are allowed access even if they are also on the blacklist.</p> <p>Entries are automatically removed from the blacklist after about a day.</p>

Updater Alerts

The following table contains a list of the various updater alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
The \$app application tried and failed \$attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage.	Warning.	<p>\$app: Web Security appliance security service name.</p> <p>\$attempts: Number of attempts tried.</p>
The updater has been unable to communicate with the update server for at least \$threshold.	Warning.	\$threshold: Threshold value time.
Unknown error occurred: \$traceback.	Critical.	\$traceback: Traceback information.

Anti-Malware Alerts

For information about alerts related to Advanced Malware Protection, see [Ensuring That You Receive Alerts, page 14-10](#).

FIPS Compliance

Federal Information Processing Standards (FIPS) specify requirements for cryptographic modules that are used by all government agencies to protect sensitive but unclassified information. FIPS help ensure compliance with federal security and data privacy requirements. FIPS, developed by the National Institute for Standards and Technology (NIST), are to use when no voluntary standards exist to meet federal requirements.

The WSA achieves FIPS 140-2 Level 1 compliance in FIPS mode using Cisco Common Cryptographic Module (C3M). By default, FIPS mode is disabled.

FIPS Certificate Requirements

FIPS mode requires that all enabled encryption services on the Web Security appliance use a FIPS-compliant certificate. This applies to the following encryption services:

- HTTPS Proxy
- Authentication
- Identity Provider for SaaS
- Appliance Management HTTPS Service



Note

The Appliance Management HTTPS Service must be enabled before FIPS mode can be enabled. The other encryption services need not be enabled.

A FIPS-compliant certificate must meet these requirements:

Certificate	Algorithm	Bit Key Size	Signature Algorithm	Notes
X509	RSA	1024, 2048, 3072, or 4096	sha1WithRSAEncryption	Cisco recommends a bit key size of 1024 for best decryption performance and sufficient security. A larger bit size will increase security, but impact decryption performance.
	DSA	1024	dsaWithSHA1	

Enabling or Disabling FIPS Mode

Before You Begin

- Ensure the certificates to be used in FIPS mode use FIPS 140-2 approved public key algorithms (see [FIPS Certificate Requirements, page 21-21](#)).



Note

Changing the FIPS mode initiates a reboot of the appliance.

- Step 1** Choose **System Administration > FIPS Mode**.
- Step 2** Click **Edit Settings**.
- Step 3** Check or uncheck the **Enable FIPS Level 1 Compliance** check box.
- Step 4** Click **Submit**.
- Step 5** Click **Continue** to allow the appliance to reboot.

System Date and Time Management

Your Web Security appliance can track the current date and time by querying a Network Time Protocol (NTP) server or you can manually set the system date and time. The system date and time reflects the time zone, which you can set either by GMT offset or by global region, country, and then local time zone.

Setting the Time Zone

-
- Step 1** Choose **System Administration > Time Zone**.
 - Step 2** Click **Edit Settings**.
 - Step 3** Select your region, country, and time zone or select the GMT offset.
 - Step 4** Submit and commit the changes.
-

Synchronizing the System Clock with an NTP Server

-
- Step 1** Choose **System Administration > Time Settings**.
 - Step 2** Click **Edit Settings**.
 - Step 3** Select **Use Network Time Protocol** as the Time Keeping Method.
 - Step 4** Enter the fully qualified hostname or IP address of the NTP server, clicking **Add Row** as needed to add servers.
 - Step 5** (Optional) Choose the routing table associated with an appliance network interface type, either Management or Data, to use for NTP queries. This is the IP address from which NTP queries should originate.



Note This option is only editable if the appliance is using split routing for data and management traffic.

- Step 6** Submit and commit your changes.
-

Deleting an NTP Server from the Configuration

-
- Step 1** Choose **System Administration > Time Settings**.
 - Step 2** Click **Edit Settings**.
 - Step 3** Click the garbage can icon to the right of the server name to delete it.
 - Step 4** Submit and commit your changes.
-

Manually Setting the System Date and Time in the GUI

-
- Step 1** Choose **System Administration > Time Settings**.
 - Step 2** Click the **Select Set Time Manually** radio button.
 - Step 3** Set the date and time.
 - Step 4** Click **Submit**.
-

Installing a Server Digital Certificate

When an administrator logs into the Web Security appliance using HTTPS, the appliance uses a digital certificate to securely establish the connection with the client application. The Web Security appliance uses the “Cisco Web Security Appliance Demo Certificate” that comes installed by default. However, client applications are not programmed to recognize this certificate, so you can upload a digital certificate to the appliance that your applications recognize automatically.

To configure the Web Security appliance to use a different digital server certificate, follow these steps:

-
- Step 1** Obtain a certificate and private key pair to upload.
 - Step 2** Upload the certificate and private key pair to the appliance.
-

Related Topics

- [Obtaining Certificates, page 21-23.](#)
- [Uploading Certificates to the Web Security Appliance, page 21-24.](#)

Obtaining Certificates

-
- Step 1** Generate a public-private key pair.
 - Step 2** Generate a Certificate Signing Request (CSR).
 - Step 3** Contact a certificate authority (CA) to sign the certificate.
-

Server Digital Certificate Requirements

The certificate you upload to the appliance must meet the following requirements:

- It must use the X.509 standard.
- It must include a matching private key in PEM format. DER format is not supported.
- The private key must be unencrypted.

Certificate Signing Requests

The Web Security appliance cannot generate Certificate Signing Requests (CSR) for certificates uploaded to the appliance. Therefore, to have a certificate created for the appliance, you must issue the signing request from another system. Save the PEM-formatted key from this system because you will need to install it on the appliance later.

You can use any UNIX machine with a recent version of OpenSSL installed. Be sure to put the appliance hostname in the CSR. Use the guidelines at the following location for information on generating a CSR using OpenSSL:

http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28

Once the CSR has been generated, submit it to a certificate authority (CA). The CA will return the certificate in PEM format.

If you are acquiring a certificate for the first time, search the Internet for “certificate authority services SSL server certificates,” and choose the service that best meets the needs of your organization. Follow the service’s instructions for obtaining an SSL certificate.

**Note**

You can also generate and sign your own certificate. Tools for doing this are included with OpenSSL, free software from <http://www.openssl.org>.

Intermediate Certificates

In addition to root certificate authority (CA) certificate verification, AsyncOS supports the use of intermediate certificate verification. Intermediate certificates are certificates issued by a trusted root CA which are then used to create additional certificates. This creates a chained line of trust. For example, a certificate may be issued by example.com who, in turn, is granted the rights to issue certificates by a trusted root CA. The certificate issued by example.com must be validated against example.com’s private key as well as the trusted root CA’s private key.

Uploading Certificates to the Web Security Appliance

Step 1 Access the CLI

Step 2 Enter the `certconfig` command.

The following example shows a certificate being uploaded. You can also add intermediate certificates from this command.

```
example.com> certconfig
```

```
Currently using the demo certificate/key for HTTPS management access.
```

```
Choose the operation you want to perform:
```

```
- SETUP - Configure security certificate and key.
```

```
[ ]> setup
```

```
Management (HTTPS):
```

```
paste cert in PEM format (end with '.'):

```

```
-----BEGIN CERTIFICATE-----

```

```
MIICLCCAdYCAQAwDQYJKoZIhvcNAQEEBQAwwAxCzAJBgNVBAYTAlBUMRMwEQYD
VQQTIEwprDwVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNib2ExFzAVBgNVBAoTDk51dXJv
bmlvLlBUMZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZG
dXR1cy5uZXVyb25pby5wdDEbMBkGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZpMB4X
DTk2MDkwNTAzNDI0M1oXDTk2MTAwNTAzNDI0M1owgaAxCzAJBgNVBAYTAlBUMRMw
EQYDVQQIEwprDwVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNib2ExFzAVBgNVBAoTDk51
dXJvbmlvLlBUMZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZG
EmJydXR1cy5uZXVyb25pby5wdDEbMBkGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZp
MFwwDQYJKoZIhvcNAQEEBQAQSwAwSAJBAL7+aty3S1iBA/+yxjxv4q1MUTd1kjNw
L4lYKbpzzlmc5beaQXeQ2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAATAN
BgkqhkiG9w0BAQQFAANBAFqPEKfjk6T6CKTHvaQeEAsX0/8YHPHqH/9Anhsjrwx
9EBc0n6bVGhN7XaXd6sJ7dym9sbsWxb+pJdurnkxjx4=

```

```
-----END CERTIFICATE-----

```

```
.
```

```
paste key in PEM format (end with '.'):

```

```
-----BEGIN RSA PRIVATE KEY-----

```

```
MIIBPAIBAAJBAL7+aty3S1iBA/+yxjxv4q1MUTd1kjNwL4lYKbpzzlmc5beaQXeQ
2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAAQJBBALjkK+jc2+iihI98riEF
oudmknZiSRTYjnwjx8mCoAJPWviB3c742e03FG4/soi1jD9A5alihEOXFUzloenr
8IECIQD3B5+01+68BA/6d76iUNqAAV8djGTzvxnCxycnxPQydQIhAMXt4trUI3nc
a+U8YL2HPFA3gmhBSiCbq2OptOCnM7hAiEA6Xi3JIQECob8Ywkrj29DU3/4WYD7
WLPgsQpwo1GuSpECICGsnWH5oaeD9t9jbFoSfhJvv0IZmxcLpRcpslpeWBBAiEA
6/5B8J0GHdJq89FHwEG/H2eVVUYu5y/aD6sgcm+0Avg=

```

```

-----END RSA PRIVATE KEY-----
.

Do you want add an intermediate certificate? [N]> N

Currently using custom certificate/key for HTTPS management access.

Choose the operation you want to perform:

- SETUP - Configure security certificate and key.

[]>

example.com> commit

Please enter some comments describing your changes:

[]> Installed certificate and key for HTTPS management.

Changes committed: Fri Sep 26 17:59:53 2008 GMT

```

AsyncOS for Web Upgrades and Updates

Cisco periodically releases upgrades (new software versions) and updates (changes to current software versions) for AsyncOS for Web and its components.

Best Practices For Upgrading AsyncOS for Web

- Before you start the upgrade, save the XML configuration file off the Web Security appliance from the System Administration > Configuration File page or by using the `saveconfig` command.
- Save other files stored on the appliance, such as PAC files or customized end-user notification pages.
- When upgrading, do not pause for long amounts of time at the various prompts. If the TCP session times out during the download, the upgrade may fail.
- After the upgrade completes, save the configuration information to an XML file.

Related Topics

- [Saving and Loading the Appliance Configuration, page 21-2.](#)

Upgrading and Updating AsyncOS and Security Service Components

Upgrading AsyncOS for Web

Before You Begin

- Save the appliance configuration file (see [Saving and Loading the Appliance Configuration, page 21-2](#)).

-
- | | |
|---------------|--|
| Step 1 | Choose System Administration > System Upgrade . |
| Step 2 | Click Available Upgrades . |
| Step 3 | Select an upgrade from the list of available upgrades, and click Begin Upgrade to start the upgrade process. Answer the questions as they appear. |
| Step 4 | When the upgrade is complete, click Reboot Now to reboot the Web Security appliance. |
-

Related Topics

- [Local And Remote Update Servers, page 21-28.](#)

Automatic and Manual Update and Upgrade Queries

AsyncOS periodically queries the update servers for new updates to all security service components, but not for new AsyncOS upgrades. To upgrade AsyncOS, you must manually prompt AsyncOS to query for available upgrades. You can also manually prompt AsyncOS to query for available security service updates. For more information, see [Reverting to a Previous Version of AsyncOS for Web, page 21-32](#).

When AsyncOS queries an update server for an update or upgrade, it performs the following steps:

1. Contacts the update server.

Cisco allows the following sources for update servers:

- **Cisco update servers.** For more information, see [Note Local update servers do not automatically receive security service updates, only AsyncOS upgrades. After using a local update server for upgrading AsyncOS, change the update and upgrade settings back to use the Cisco update servers so the security services update automatically again., page 21-28.](#)
 - **Local server.** For more information, see [Upgrading from a Local Server, page 21-29.](#)
2. Receives an XML file that lists the available updates or AsyncOS upgrade versions. This XML file is known as the “manifest.”
 3. Downloads the update or upgrade image files.

Manually Updating Security Service Components

By default, each security service component periodically receives updates to its database tables from the Cisco update servers. However, you can manually update the database tables.

**Note**

Some updates are available on an on-demand basis from the GUI pages related to the feature.

-
- Step 1** Choose **System Administration > Upgrade and Update Settings**.
- Step 2** Click **Edit Update Settings**.
- Step 3** Specify the location of the update files.
- Step 4** Initiate the update using the Update Now function key on the component page located on the Security Services tab. For example, Security Services > Web Reputation Filters page.

**Note**

Updates that are in-progress cannot be interrupted. All in-progress updates must complete before new changes can be applied.

**Tip**

View a record of update activity in the updater log file. Subscribe to the updater log file on the System Administration > Log Subscriptions page.

Local And Remote Update Servers

By default, AsyncOS contacts the Cisco update servers for both update and upgrade images and the manifest XML file. However, you can choose from where to download the upgrade and update images and the manifest file. Using a local update server for the images or manifest file for any of the following reasons:

- **You have multiple appliances to upgrade simultaneously.** You can download the upgrade image to a web server inside your network and serve it to all appliances in your network.
- **Your firewall settings require static IP addresses for the Cisco update servers.** The Cisco update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for updates and AsyncOS upgrades. For more information, see [Configuring a Static Address for the Cisco Update Servers, page 21-29](#).

**Note**

Local update servers do not automatically receive security service updates, only AsyncOS upgrades. After using a local update server for upgrading AsyncOS, change the update and upgrade settings back to use the Cisco update servers so the security services update automatically again.

Updating and Upgrading from the Cisco Update Servers

A Web Security appliance can connect directly to Cisco update servers and download upgrade images and security service updates. Each appliance downloads the updates and upgrade images separately.

Configuring a Static Address for the Cisco Update Servers

The Cisco update servers use dynamic IP addresses. If you have strict firewall policies, you may need to configure a static location for updates and AsyncOS upgrades.

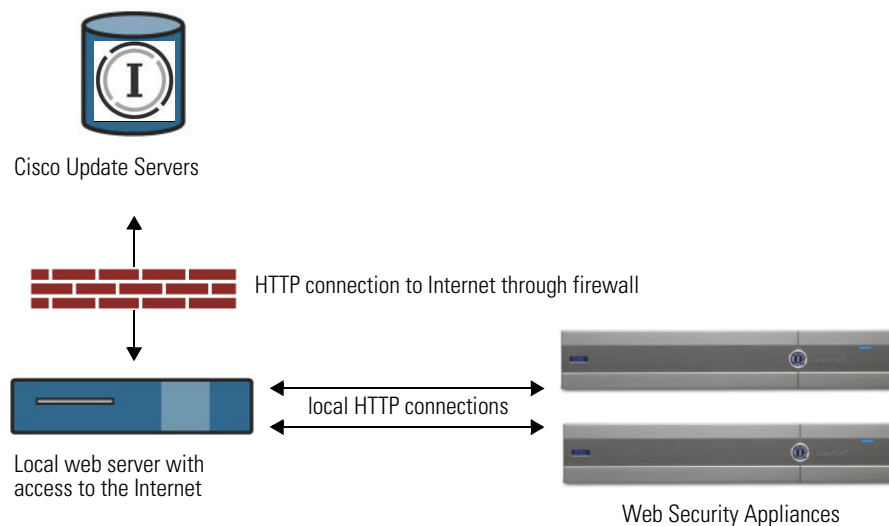
-
- Step 1** Contact Cisco Customer Support to obtain the static URL address.
 - Step 2** Navigate to the System Administration > Upgrade and Update Settings page, and click **Edit Update Settings**.
 - Step 3** On the Edit Update Settings page, in the “Update Servers (images)” section, choose Local Update Servers and enter the static URL address received in step 1.
 - Step 4** Verify that Cisco Update Servers is selected for the “Update Servers (list)” section.
 - Step 5** Submit and commit your changes.
-

Upgrading from a Local Server

The Web Security appliance can download AsyncOS upgrades from a server within your network instead of obtaining upgrades directly from the Cisco update servers. When you use this feature, you download the upgrade image from Cisco once only, and then serve it to all Web Security appliances in your network.

Figure 21-2 shows how Web Security appliances download upgrade images from local servers.

Figure 21-2 Upgrading from a Local Server



Hardware and Software Requirements for Local Upgrade Servers

For *downloading* AsyncOS upgrade files, you must have a system in your internal network that has a web browser and Internet access to the Cisco update servers.

**Note**

If you need to configure a firewall setting to allow HTTP access to this address, you must configure it using the DNS name and not a specific IP address.

For *hosting* AsyncOS upgrade files, a server on the internal network must have a web server, such as Microsoft IIS (Internet Information Services) or the Apache open source server, which has the following features:

- Supports the display of directory or filenames in excess of 24 characters.
- Has directory browsing enabled.
- Is configured for anonymous (no authentication) or Basic (“simple”) authentication.
- Contains at least 350MB of free disk space for each AsyncOS upgrade image.

Configuring Upgrades from a Local Server

- Step 1** Configure a local server to retrieve and serve the upgrade files.
- Step 2** Download the upgrade zip file.
- Using a browser on the local server, go to http://updates.ironport.com/fetch_manifest.html to download a zip file of an upgrade image. To download the image, enter your serial number (for a physical appliance) or VLN (for a virtual appliance) and the version number of the appliance. You will then be presented with a list of available upgrades. Click on the upgrade version that you want to download.
- Step 3** Unzip the zip file in the root directory on the local server while keeping the directory structure intact.
- Step 4** Configure the appliance to use the local server using the System Administration > Upgrade and Update Settings page or the `updateconfig` command.
- Step 5** On the System Administration > System Upgrade page, click **Available Upgrades** or run the `upgrade` command.
-

**Note**

Cisco recommends changing the update and upgrade settings to use the Cisco update servers (using dynamic or static addresses) after the upgrade is complete to ensure the security service components continue to update automatically.

Differences Between Local and Remote Upgrading Methods

The following differences apply when upgrading AsyncOS from a local server rather than from a Cisco update server:

1. The upgrading installs immediately *while downloading*.
2. A banner displays for 10 seconds at the beginning of the upgrade process. While this banner is displayed, you have the option to type Control+C to exit the upgrade process before downloading starts.

Configuring Upgrade and Service Update Settings

You can configure how the Web Security appliance downloads security services updates and AsyncOS for Web upgrades. For example, you can choose which network interface to use when downloading the files, configure the update interval or disable automatic updates.

Step 1 Choose **System Administration > Upgrade and Update Settings**.

Step 2 Click **Edit Update Settings**.

Step 3 Configure the settings, referencing the following information:

Setting	Description
Automatic Updates	Choose whether or not to enable automatic updates of the security components. If you choose automatic updates, enter the time interval. The default is enabled and the update interval is 5 minutes.
Upgrade Notifications	Choose whether to display a notification at the top of the Web Interface when a new upgrade to AsyncOS is available. The appliance only displays this notification for administrators. For more information, see Upgrading AsyncOS for Web, page 21-27 .
Update Servers (list)	Whether to download the list of available upgrades and updates (the manifest XML file) from the Cisco update servers or a local web server. When you choose a local update server, enter the full path to the manifest XML file for the list including the file name and port number for the server. If you leave the port field blank, AsyncOS uses port 80. If the server requires authentication, you can also enter a valid user name and password.
Update Servers (images)	Whether to download upgrade and update images from the Cisco update servers or a local web server. When you choose a local update server, enter the base URL and port number for the server. If you leave the port field blank, AsyncOS uses port 80. If the server requires authentication, you can also enter a valid user name and password.
Routing Table	Choose which network interface's routing table to use when contacting the update servers.
Proxy Server (optional)	If an upstream proxy server exists and requires authentication, enter the server information and user name and password here.

Step 4 Submit and commit your changes.

Related Topics

- [Local And Remote Update Servers, page 21-28](#).
- [Automatic and Manual Update and Upgrade Queries, page 21-27](#).
- [Upgrading and Updating AsyncOS and Security Service Components, page 21-27](#).

Reverting to a Previous Version of AsyncOS for Web

AsyncOS for Web supports the ability to revert the AsyncOS for Web operating system to a previous qualified build for emergency uses.

**Note**

You cannot revert to a version of AsyncOS for Web earlier than version 7.5.

Configuration File Use in the Revert Process

Effective in version 7.5, when you upgrade to a later version, the upgrade process automatically saves the current system configuration to a file on the Web Security appliance. (However, Cisco recommends manually saving the configuration file to a local machine as a backup.) This allows AsyncOS for Web to load the configuration file associated with the earlier release after reverting to the earlier version. However, when it performs a reversion, it uses the current network settings for the management interface.

Reverting AsyncOS for an Appliance Managed by the SMA

You can revert AsyncOS for Web from the Web Security appliance. However, if the Web Security appliance is managed by a Security Management appliance, consider the following rules and guidelines:

- When Centralized Reporting is enabled on the Web Security appliance, AsyncOS for Web finishes transferring the reporting data to the Security Management appliance before it starts the reversion. If the files take longer than 40 seconds to transfer to the Security Management appliance, AsyncOS for Web prompts you to continue waiting to transfer the files, or continue the reversion without transferring all files.
- You must associate the Web Security appliance with the appropriate Configuration Master after reverting. Otherwise, pushing a configuration from the Security Management appliance to the Web Security appliance might fail.

Reverting AsyncOS for Web to a Previous Version

**Warning**

Reverting the operating system on a Web Security appliance is a very destructive action and destroys all configuration logs and databases. Reversion also disrupts web traffic handling until the appliance is reconfigured. Depending on the initial Web Security appliance configuration, this action may destroy network configuration. If this happens, you will need physical local access to the appliance after performing the reversion.

Before You Begin

- Contact Cisco Quality Assurance to confirm that you can perform the intended reversion.
- Back up the following information from the Web Security appliance to a separate machine:
 - System configuration file (with passwords unmasked).
 - Log files you want to preserve.
 - Reports you want to preserve.

- Customized end-user notification pages stored on the appliance.
- PAC files stored on the appliance.

Step 1 Log into the CLI of the appliance you want to revert.



Note When you run the `revert` command in the next step, several warning prompts are issued. After these warning prompts are accepted, the revert action takes place immediately. Therefore, do not begin the reversion process until after you have completed the pre-reversion steps.

Step 2 Enter the `revert` command.

Step 3 Confirm twice that you want to continue with the reversion.

Step 4 Choose one of the available versions to revert to.

The appliance reboots twice.



Note The reversion process is time-consuming. It may take fifteen to twenty minutes before reversion is complete and console access to the appliance is available again.

The appliance should now run using the selected AsyncOS for Web version. You can access the web interface from a web browser.



Note If updates to the set of URL categories are available, they will be applied after AsyncOS reversion



Troubleshooting

- [Authentication Problems](#)
- [Blocked Object Problems](#)
- [Browser Problems](#)
- [DNS Problems](#)
- [Feature Keys Expired](#)
- [FTP Problems](#)
- [HTTPS/Decryption/Certificate Problems](#)
- [Logging Problems](#)
- [Policy Problems](#)
- [Problems with File Reputation and File Analysis](#)
- [Site Access Problems](#)
- [Upstream Proxy Problems](#)
- [WCCP Problems](#)

Authentication Problems

- [LDAP Problems](#)
- [Basic Authentication Problems](#)
- [Single Sign-On Problems](#)
- Also see:
 - [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication](#)
 - [Cannot Access URLs that Do Not Support Authentication](#)
 - [Client Requests Fail Upstream Proxy](#)

LDAP Problems

- [LDAP User Fails Authentication due to NTLMSSP](#)
- [LDAP Authentication Fails due to LDAP Referral](#)

LDAP User Fails Authentication due to NTLMSSP

LDAP servers do not support NTLMSSP. Some client applications, such as Internet Explorer, always choose NTLMSSP when given a choice between NTLMSSP and Basic. When all of the following conditions are true, the user will fail authentication:

- The user only exists in the LDAP realm.
- The Identity uses a sequence that contains both LDAP and NTLM realms.
- The Identity uses the “Basic or NTLMSSP” authentication scheme.
- A user sends a request from an application that chooses NTLMSSP over Basic.

Reconfigure the identity or the authentication realm or the application such that at least one of the above conditions will be false.

LDAP Authentication Fails due to LDAP Referral

LDAP authentication fails when all of the following conditions are true:

- The LDAP authentication realm uses an Active Directory server.
- The Active Directory server uses an LDAP referral to another authentication server.
- The referred authentication server is unavailable to the Web Security appliance.

Workarounds:

- Specify the Global Catalog server (default port is 3268) in the Active Directory forest when you configure the LDAP authentication realm in the appliance,
- Use the `advancedproxyconfig > authentication` CLI command to disable LDAP referrals. LDAP referrals are disabled by default.

Basic Authentication Problems

- [Basic Authentication Fails](#)

Related Problems

- [Upstream Proxy Does Not Receive Basic Credentials](#)

Basic Authentication Fails

AsyncOS for Web only supports 7-bit ASCII characters for passwords when using the Basic authentication scheme. Basic authentication fails when the password contains characters that are not 7-bit ASCII.

Single Sign-On Problems

- [Users Erroneously Prompted for Credentials](#)

Users Erroneously Prompted for Credentials

NTLM authentication does not work in some cases when the Web Security appliance is connected to a WCCP v2 capable device. When a user makes a request with a highly locked down version of Internet Explorer that does not do transparent NTLM authentication correctly and the appliance is connected to a WCCP v2 capable device, the browser defaults to Basic authentication. This results in users getting prompted for their authentication credentials when they should not get prompted.

Workaround

In Internet Explorer, add the Web Security appliance redirect hostname to the list of trusted sites in the Local Intranet zone (Tools > Internet Options > Security tab).

Browser Problems

WPAD Not Working With Firefox

Firefox browsers may not support DHCP lookup with WPAD. For current information, see https://bugzilla.mozilla.org/show_bug.cgi?id=356831.

To use Firefox (or any other browser that does not support DHCP) with WPAD when the PAC file is hosted on the Web Security appliance, configure the appliance to serve the PAC file through port 80.

-
- Step 1** Choose **Security Services > Web Proxy** and delete port 80 from the **HTTP Ports to Proxy** field.
 - Step 2** Use port 80 as the PAC Server Port when you upload the file to the appliance.
 - Step 3** If any browsers are manually configured to point to the web proxy on port 80, reconfigure those browsers to point to another port in the HTTP Ports to Proxy field.
 - Step 4** Change any references to port 80 in PAC files.
-

DNS Problems

Alert: Failed to Bootstrap the DNS Cache

If an alert with the message “Failed to bootstrap the DNS cache” is generated when an appliance is rebooted, it means that the system was unable to contact its primary DNS servers. This can happen at boot time if the DNS subsystem comes online before network connectivity is established. If this message appears at other times, it could indicate network issues or that the DNS configuration is not pointing to a valid server.

Feature Keys Expired

If the feature key for the feature you are trying to access (via the web interface) has expired, please contact your Cisco representative or support organization.

FTP Problems

- [URL Categories Do Not Block Some FTP Sites](#)
- [Large FTP Transfers Disconnect](#)
- [Zero Byte File Appears On FTP Servers After File Upload](#)
- Also see:
 - [Unable to Route FTP Requests Via an Upstream Proxy](#)
 - [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication](#)

URL Categories Do Not Block Some FTP Sites

When a native FTP request is transparently redirected to the FTP Proxy, it contains no hostname information for the FTP server, only its IP address. Because of this, some predefined URL categories and Web Reputation Filters that have only hostname information will not match native FTP requests, even if the requests are destined for those servers. If you wish to block access to these sites, you must create custom URL categories for them using their IP addresses.

Large FTP Transfers Disconnect

If the connection between the FTP Proxy and the FTP server is slow, uploading a large file may take a long time, particularly when Cisco Data Security Filters are enabled. This can cause the FTP client to time out before the FTP Proxy uploads the entire file and you may get a failed transaction notice. The transaction does not fail, however, but continues in the background and will be completed by the FTP Proxy.

You can workaroud this issue by increasing the appropriate idle timeout value on the FTP client.

Zero Byte File Appears On FTP Servers After File Upload

FTP clients create a zero byte file on FTP servers when the FTP Proxy blocks an upload due to outbound anti-malware scanning.

HTTPS/Decryption/Certificate Problems

- [Accessing HTTPS Sites Using Routing Policies with URL Category Criteria](#)
- [HTTPS Request Failures](#)
- [Bypassing Decryption for Particular Websites](#)

- [Alert: Problem with Security Certificate](#)
- Also see:
 - [Logging HTTPS Transactions](#)
 - [Access Policy not Configurable for HTTPS](#)
 - [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication](#)

Accessing HTTPS Sites Using Routing Policies with URL Category Criteria

For transparently redirected HTTPS requests, the Web Proxy must contact the destination server to determine the server name and therefore the URL category in which it belongs. Due to this, when the Web Proxy evaluates Routing Policy Group membership, it cannot yet know the URL category of an HTTPS request because it has not yet contacted the destination server. If the Web Proxy does not know the URL category, it cannot match the transparent HTTPS request to a Routing Policy that uses a URL category as membership criteria.

As a result, transparently redirected HTTPS transactions only match Routing Policies that do not define Routing Policy Group membership criteria by URL category. If all user-defined Routing Policies define their membership by URL category, transparent HTTPS transactions match the Default Routing Policy Group.

HTTPS Request Failures

- [HTTPS with IP-based Surrogates and Transparent Requests](#)

HTTPS with IP-based Surrogates and Transparent Requests

If the HTTPS request comes from a client that does not have authentication information available from an earlier HTTP request, AsyncOS either fails the HTTPS request or decrypts the HTTPS request in order to authenticate the user, depending on how you configure the HTTPS Proxy. Use the HTTPS Transparent Request setting on the Security Services > HTTPS Proxy page to define this behavior. Refer to the Enabling HTTPS Proxy section in Decryption Policies chapter.

Bypassing Decryption for Particular Websites

Some HTTPS servers do not work as expected when traffic to them is decrypted by a proxy server, such as the Web Proxy. For example, some websites and their associated web applications and applets, such as high security banking sites, maintain a hard-coded list of trusted certificates instead of relying on the operating system certificate store.

You can bypass decryption for HTTPS traffic to these servers to ensure all users can access these types of sites.

-
- Step 1** Create a custom URL category that contains the affected HTTPS servers by configuring the Advanced properties.

- Step 2** Create a Decryption Policy that uses the custom URL category created in [Step 1](#) as part of its membership, and set the action for the custom URL category to Pass Through.
-

Alert: Problem with Security Certificate

Typically, the root certificate information you generate or upload in the appliance is not listed as a trusted root certificate authority in client applications. By default in most web browsers, when users send HTTPS requests, they will see a warning message from the client application informing them that there is a problem with the website's security certificate. Usually, the error message says that the website's security certificate was not issued by a trusted certificate authority or the website was certified by an unknown authority. Some other client applications do not show this warning message to users nor allow users to accept the unrecognized certificate.



Note **Mozilla Firefox browsers:** The certificate you upload must contain “basicConstraints=CA:TRUE” to work with Mozilla Firefox browsers. This constraint allows Firefox to recognize the root certificate as a trusted root authority.

Logging Problems

- [Custom URL Categories Not Appearing in Access Log Entries](#)
- [Logging HTTPS Transactions](#)
- [Alert: Unable to Maintain the Rate of Data Being Generated](#)
- [Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs](#)

Custom URL Categories Not Appearing in Access Log Entries

When a web access policy group has a custom URL category set to Monitor and some other component, such as the Web Reputation Filters or the DVS engine, makes the final decision to allow or block a request for a URL in the custom URL category, then the access log entry for the request shows the predefined URL category instead of the custom URL category.

Logging HTTPS Transactions

HTTPS transactions in the access logs appear similar to HTTP transactions, but with slightly different characteristics. What gets logged depends on whether the transaction was explicitly sent or transparently redirected to the HTTPS Proxy:

- **TUNNEL.** This gets written to the access log when the HTTPS request was transparently redirected to the HTTPS Proxy.
- **CONNECT.** This gets written to the access log when the HTTPS request was explicitly sent to the HTTPS Proxy.

When HTTPS traffic is decrypted, the access logs contain two entries for a transaction:

- TUNNEL or CONNECT depending on the type of request processed.

- The HTTP Method and the decrypted URL. For example, “GET https://ftp.example.com”.
- The full URL is only visible when the HTTPS Proxy decrypts the traffic.

Alert: Unable to Maintain the Rate of Data Being Generated

AsyncOS for Web sends a critical email message to the configured alert recipients when the internal logging process drops web transaction events due to a full buffer.

By default, when the Web Proxy experiences a very high load, the internal logging process buffers events to record them later when the Web Proxy load decreases. When the logging buffer fills completely, the Web Proxy continues to process traffic, but the logging process does not record some events in the access logs or in the Web Tracking report. This might occur during a spike in web traffic.

However, a full logging buffer might also occur when the appliance is over capacity for a sustained period of time. AsyncOS for Web continues to send the critical email messages every few minutes until the logging process is no longer dropping data.

The critical message contains the following text:

```
Reporting Client: The reporting system is unable to maintain the rate of data being
generated. Any new data generated will be lost.
```

If AsyncOS for Web sends this critical message continuously or frequently, the appliance might be over capacity. Contact Cisco Customer Support to verify whether or not you need additional Web Security appliance capacity.

Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs

If you want to use a third party log analyzer tool to read and parse the W3C access logs, you might need to include the “timestamp” field. The timestamp W3C field displays time since the UNIX epoch, and most log analyzers only understand time in this format.

Policy Problems

- [Access Policy not Configurable for HTTPS](#)
- [Blocked Object Problems](#)
- [Identity Disappeared from Policy](#)
- [Policy Match Failures](#)
- [Policy Troubleshooting Tool: Policy Trace](#)
- Also see: [Accessing HTTPS Sites Using Routing Policies with URL Category Criteria](#)

Access Policy not Configurable for HTTPS

With the HTTPS Proxy is enabled, Decryption Policies handle all HTTPS policy decisions. You can no longer define Access and Routing Policy group membership by HTTPS, nor can you configure Access Policies to block HTTPS transactions.

If some Access and Routing Policy group memberships are defined by HTTPS and if some Access Policies block HTTPS, then when you enable the HTTPS Proxy, those Access and Routing Policy groups become disabled. You can choose to enable the policies at any time, but all HTTPS related configurations are removed.

Blocked Object Problems

- [Some Microsoft Office Files Not Blocked](#)
- [Blocking DOS Executable Object Types Blocks Updates for Windows OneCare](#)

Some Microsoft Office Files Not Blocked

When you block Microsoft Office files in the Block Object Type section, it is possible that some Microsoft Office files will not be blocked.

If you need to block all Microsoft Office files, add `application/x-ole` in the Block Custom MIME Types field. However, blocking this custom MIME type also blocks all Microsoft Compound Object format types, such as Visio files and some third party applications.

Blocking DOS Executable Object Types Blocks Updates for Windows OneCare

When you configure the Web Security appliance to block DOS executable object types, the appliance also blocks updates for Windows OneCare.

Identity Disappeared from Policy

Deleting an authentication realm disables associated identities. Disabling an identity removes it from associated policies. Verify that the identity is enabled and then add it to the policy again.

Policy Match Failures

- [Policy is Never Applied](#)
- [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication](#)
- [User Matches Global Policy for HTTPS and FTP over HTTP Requests](#)
- [User Assigned Incorrect Access Policy](#)

Policy is Never Applied

If multiple Identities have identical criteria, AsyncOS assigns the transactions to the first identity that matches. Therefore, transactions never match the additional, identical identities. Any policies that apply to those subsequent, identical identities are never matched or applied.

HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication

Configure the appliance to use IP addresses as the surrogate when credential encryption is enabled.

When credential encryption is enabled and configured to use cookies as the surrogate type, authentication does not work with HTTPS or FTP over HTTP requests. This is because the Web Proxy redirects clients to the Web Proxy itself for authentication using an HTTPS connection if credential encryption is enabled. After successful authentication, the Web Proxy redirects clients back to the original website. In order to continue to identify the user, the Web Proxy must use a surrogate (either the IP address or a cookie). However, using a cookie to track users results in the following behavior if requests use HTTPS or FTP over HTTP:

- **HTTPS.** The Web Proxy must resolve the user identity before assigning a Decryption Policy (and therefore, decrypt the transaction), but it cannot obtain the cookie to identify the user unless it decrypts the transaction.
- **FTP over HTTP.** The dilemma with accessing FTP servers using FTP over HTTP is similar to accessing HTTPS sites. The Web Proxy must resolve the user identity before assigning an Access Policy, but it cannot set the cookie from the FTP transaction.

Therefore, HTTPS and FTP over HTTP requests will match only Access Policies that do not require authentication. Typically, they match the global Access Policy because it never requires authentication.

User Matches Global Policy for HTTPS and FTP over HTTP Requests

When the appliance uses cookie-based authentication, the Web Proxy does not get cookie information from clients for HTTPS and FTP over HTTP requests. Therefore, it cannot get the user name from the cookie.

HTTPS and FTP over HTTP requests still match the Identity according to the other membership criteria, but the Web Proxy does not prompt clients for authentication even if the Identity requires authentication. Instead, the Web Proxy sets the user name to NULL and considers the user as unauthenticated.

Then, when the unauthenticated request is evaluated against a policy, it matches only a policy that specifies “All Identities” and apply to “All Users.” Typically, this is the global policy, such as the global Access Policy.

User Assigned Incorrect Access Policy

- Clients on your network use Network Connectivity Status Indicator (NCSI)
- Web Security appliance uses NTLMSSP authentication.
- Identity uses IP based surrogates

A user might be identified using the machine credentials instead of the user’s own credentials, and as a result, might be assigned to an incorrect Access Policy.

Workaround:

- Reduce the surrogate timeout value for machine credentials.

Step 1 Use the `advancedproxyconfig > authentication` CLI command.

Step 2 Enter the surrogate timeout for machine credentials.

Policy Troubleshooting Tool: Policy Trace

- [About the Policy Trace Tool](#)
- [Tracing Client Requests](#)
- [Customizing Request Details](#)
- [Overriding Response Details](#)

About the Policy Trace Tool

The Policy Trace Tool can emulate a client request and then detail how the Web Proxy processes that request. It can be used to trace client requests and debug policy processing when troubleshooting Web Proxy issues. You may perform a basic trace or you may enter advanced trace settings and override options.

The policy trace tool evaluates requests against polices used by the Web Proxy only. These are Access, Encrypted HTTPS Management, Routing, Data Security, and Outbound Malware Scanning polices.


Note

SOCKS and External DLP polices are not evaluated by the policy trace tool.


Note

When you use the policy trace tool, the Web Proxy does not record the requests in the access log or reporting database

Tracing Client Requests

- Step 1** Choose **System Administration > Policy Trace**.
- Step 2** Enter the URL you wish to trace to in the URL field.
- Step 3** (Optional) Enter additional emulation parameters:

Table A-1

To emulate...	Enter...
The client source IP used to make the request.	An IP address in the Client IP Address field. Note If no IP address is specified, AsyncOS uses localhost
The authentication credentials used to make the request.	A user name in the User Name field and select an authentication realm in the Authentication Realm drop-down list. Note For authentication to work for the user you enter here, the user must have already successfully authenticated through the Web Security appliance.

- Step 4** Click **Find Policy Match**.

The policy trace output is displayed in the Results pane.

Customizing Request Details

Step 1 Expand the **Advanced** section within the Policy Trace page.

Step 2 Complete the fields in the Request Details pane as required:.

Table A-2

Setting	Description
Proxy Port	Select a specific proxy port to use for the trace request to test policy membership based on proxy port.
Client Application	Specify the client application to simulate in the request.
Time of Request	Specify the day of week and time of day to simulate in the request.
Upload File	Choose a local file to simulate uploading in the request. When you specify a file to upload here, the Web Proxy simulates an HTTP POST request instead of a GET request.
Object Size	Enter the size of the request object in bytes. You can enter K, M, or G to represent Kilobytes, Megabytes, or Gigabytes.
MIME Type	Enter the MIME type.
Anti-malware Scanning Verdicts	Choose whether or not to override the Webroot, McAfee, or Sophos scanning verdicts.

Step 3 Click **Find Policy Match**.

The policy trace output is displayed in the Results pane.

Overriding Response Details

Step 1 Expand the **Advanced** section within the Policy Trace page.

Step 2 Complete the fields in the Response Detail Overrides pane as required:

Table A-3

Setting	Description
URL Category	Choose whether or not to override the URL category of the transaction response.
Application	Choose an application that the Application Visibility and Control engine can detect.

Table A-3

Setting	Description
Object Size	Enter the size of the response object in bytes. You can enter K, M, or G to represent Kilobytes, Megabytes, or Gigabytes.
MIME Type	Enter the MIME type.
Web Reputation Score	Enter the web reputation score from -10.0 to 10.0.
Anti-malware Scanning Verdicts	Choose whether or not to override the Webroot, McAfee, or Sophos scanning verdicts.

Step 3 Click **Find Policy Match**.

The policy trace output is displayed in the Results pane.

Problems with File Reputation and File Analysis

See [Troubleshooting File Reputation and Analysis](#), page 14-15.

Site Access Problems

- [Cannot Access URLs that Do Not Support Authentication](#)
- [Cannot Access Sites With POST Requests](#)
- Also see: [Bypassing Decryption for Particular Websites](#)

Cannot Access URLs that Do Not Support Authentication

This is a partial list of applications cannot be used when the Web Security appliance is deployed in transparent mode because they do not support authentication.

- Mozilla Thunderbird
- Adobe Acrobat Updates
- HttpBridge
- Subversion, by CollabNet
- Microsoft Windows Update
- Microsoft Visual Studio

Workaround: Create a class of user for the URL that does not require authentication.

Related Topics

- [Bypassing Authentication](#), page 6-20

Cannot Access Sites With POST Requests

When the user's first client request is a POST request and the user still needs to authenticate, the POST body content is lost. This might be a problem when the POST request is for an application with the Access Control single sign-on feature in use.

Workarounds:

- Have users first authenticate with the Web Proxy by requesting a different URL through the browser before connecting to a URL that uses POST as a first request.
- Bypass authentication for URLs that use POST as a first request.



Note When working with Access Control, you can bypass authentication for the Assertion Consumer Service (ACS) URL configured in the Application Authentication Policy.

Related Topics

- [Bypassing Authentication, page 6-20.](#)

Upstream Proxy Problems

- [Upstream Proxy Does Not Receive Basic Credentials](#)
- [Client Requests Fail Upstream Proxy](#)

Upstream Proxy Does Not Receive Basic Credentials

If both the appliance and the upstream proxy use authentication with NTLMSSP, depending on the configurations, the appliance and upstream proxy might engage in an infinite loop of requesting authentication credentials. For example, if the upstream proxy requires Basic authentication, but the appliance requires NTLMSSP authentication, then the appliance can never successfully pass Basic credentials to the upstream proxy. This is due to limitations in authentication protocols.

Client Requests Fail Upstream Proxy

Configuration:

- Web Security appliance and upstream proxy server use Basic authentication.
- Credential Encryption is enabled on the downstream Web Security appliance.

Client requests fail on the upstream proxy because the Web Proxy receives an "Authorization" HTTP header from clients, but the upstream proxy server requires a "Proxy-Authorization" HTTP header.

Unable to Route FTP Requests Via an Upstream Proxy

If your network contains an upstream proxy that does not support FTP connections, then you must create a Routing Policy that applies to all Identities and to just FTP requests. Configure that Routing Policy to directly connect to FTP servers or to connect to a proxy group whose proxies all support FTP connections.

WCCP Problems

Maximum Port Entries

In deployments using WCCP, the maximum number of port entries is 30 for HTTP, HTTPS , and FTP ports combined.



Command Line Interface

- [Overview of the Command Line Interface, page 27-1](#)
- [Accessing the Command Line Interface, page 27-1](#)
- [General Purpose CLI Commands, page 27-4](#)
- [Web Security Appliance CLI Commands, page 27-6](#)

Overview of the Command Line Interface

The AsyncOS Command Line Interface (CLI) allows you to configure and monitor the Web Security appliance. The Command Line Interface is accessible using SSH on IP interfaces that have been configured with these services enabled, or using terminal emulation software on the serial port. By default, SSH is configured on the Management port.

The commands are invoked by entering the command name with or without any arguments. If you enter a command without arguments, the command prompts you for the required information.

Accessing the Command Line Interface

You can add other users with differing levels of permission after you have accessed the CLI for the first time using the admin account. The System Setup Wizard prompts you to change the password for the admin account.

You can also reset the admin account password at any time using the `passwd` command.

You can connect using one of the following methods:

- **Ethernet.** Start an SSH session with the IP address of the Web Security appliance. The factory default IP address is 192.168.42.42. SSH is configured to use port 22.
- **Serial connection.** Start a terminal session with the communication port on your personal computer that the serial cable is connected to.

Log in to the appliance by entering the username and password below.

- Username: `admin`
- Password: `ironport`

Working with the Command Prompt

The top-level command prompt consists of the fully qualified hostname, followed by the greater than (>) symbol, followed by a space. For example:

```
example.com>
```

When running commands, the CLI requires input from you. When the CLI is expecting input, the prompt displays the default values enclosed in square brackets ([]) followed by the greater than (>) symbol. When there is no default value, the brackets are empty.

For example:

```
example.com> routeconfig
```

```
Choose a routing table:  
- MANAGEMENT - Routes for Management Traffic  
- DATA - Routes for Data Traffic  
[]>
```

When there is a default setting, the setting is displayed within the command-prompt brackets. For example:

```
example.com> setgateway
```

```
Warning: setting an incorrect default gateway may cause the current connection  
to be interrupted when the changes are committed.  
Enter new default gateway:  
[172.xx.xx.xx]>
```

When a default setting is shown, typing Return is equivalent to accepting the default:

Command Syntax

When operating in the interactive mode, the CLI command syntax consists of single commands with no white space and no arguments or parameters. For example:

```
example.com> logconfig
```

Select Lists

When you are presented with multiple choices for input, some commands use numbered lists. Enter the number of the selection at the prompt.

For example:

```
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 3
```

Yes/No Queries

When given a yes or no option, the question is posed with a default in brackets. You may answer **y**, **n**, **yes**, or **no**. Case is not significant.

For example:

```
Do you want to enable the proxy? [Y]> Y
```

Subcommands

Some commands give you the opportunity to use subcommand directives such as **NEW**, **EDIT**, and **DELETE**. The **EDIT** and **DELETE** functions provide a list of previously configured values.

For example:

```
example.com> interfaceconfig

Currently configured interfaces:

1. Management (172.xxx.xx.xx/xx: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.

[]>
```

Within subcommands, typing Enter or Return at an empty prompt returns you to the main command.

Escaping Subcommands

You can use the Ctrl+C keyboard shortcut at any time within a subcommand to immediately exit return to the top level of the CLI.

Command History

The CLI keeps a history of all commands entered during a session. Use the Up and Down arrow keys on your keyboard, or the Ctrl+P and Ctrl+N key combinations to scroll through a running list of the recently-used commands.

Completing Commands

The AsyncOS CLI supports command completion. You can enter the first few letters of some commands followed by the Tab key and the CLI completes the string. If the letters you entered are not unique among commands, the CLI “narrows” the set. For example:

```
example.com> set (type the Tab key)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth (typing the Tab again completes the entry with sethostname)
```

Committing Configuration Changes

Configuration changes do not take effect until you commit them. You can make configuration changes while web operations proceed as normal.

-
- Step 1** Issue the `commit` command at the command prompt.
 - Step 2** Give the `commit` command the input required.
 - Step 3** Receive confirmation of the `commit` procedure at the CLI.
-



Note

Changes to configuration that have not been committed are recorded, but do not go into effect until you run the `commit` command. However, not all commands require the `commit` command to be run. Exiting the CLI session, system shutdown, reboot, failure, or issuing the `clear` command clears changes that have not yet been committed.

General Purpose CLI Commands

This section describes some basic commands you might use in a typical CLI session, such as committing and clearing changes.

Committing Configuration Changes

The `commit` command allows you to change configuration settings while other operations proceed normally. Changes are not actually committed until you receive confirmation and a timestamp. Exiting the CLI session, system shutdown, reboot, failure, or issuing the `clear` command clears changes that have not yet been committed.

Entering comments after the commit command is optional.

```
example.com> commit
```

```
Please enter some comments describing your changes:
```

```
[ ]> Changed "psinet" IP Interface to a different IP address
```

```
Changes committed: Wed Jan 01 12:00:01 2007
```

**Note**

To successfully commit changes, you must be at the top-level command prompt. Type **Return** at an empty prompt to move up one level in the command line hierarchy.

Clearing Configuration Changes

The `clear` command clears any changes made to the appliance configuration since the last `commit` or `clear` command was issued.

```
example.com> clear
```

```
Are you sure you want to clear all changes since the last commit? [Y]> y
```

```
Changes cleared: Wed Jan 01 12:00:01 2007
```

```
example.com>
```

Exiting the Command Line Interface Session

The `exit` command logs you out of the CLI application. Configuration changes that have not been committed are cleared.

```
example.com> exit
```

```
Configuration changes entered but not committed. Exiting will lose changes.
```

```
Type 'commit' at the command prompt to commit changes.
```

```
Are you sure you wish to exit? [N]> y
```

Seeking Help on the Command Line Interface

The `help` command lists all available CLI commands and gives a brief description of each command. The `help` command can be invoked by typing either `help` or a single question mark (?) at the command prompt.

```
example.com> help
```

Related topics

- [Web Security Appliance CLI Commands, page 27-6.](#)

Web Security Appliance CLI Commands

The Web Security Appliance CLI supports a set of proxy and UNIX commands to access, upgrade, and administer the system.

Command	Description
<code>advancedproxyconfig</code>	Configure more advanced Web Proxy configurations, such as authentication and DNS parameters.
<code>adminaccessconfig</code>	You can configure the Web Security appliance to have stricter access requirements for administrators logging into the appliance.
<code>alertconfig</code>	Specify alert recipients, and set parameters for sending system alerts.
<code>authcache</code>	Allows you to delete one or all entries (users) from the authentication cache. You can also list all users currently included in the authentication cache.
<code>bwcontrol</code>	Enable bandwidth control debug messages in the Default Proxy log file.
<code>certconfig</code>	Configure security certificates and keys.
<code>clear</code>	Clears pending configuration changes since last commit.
<code>commit</code>	Commits pending changes to the system configuration.
<code>createcomputerobject</code>	Creates a computer object at the location you specify.
<code>datasecurityconfig</code>	Defines a minimum request body size, below which upload requests are not scanned by the Cisco IronPort Data Security Filters.
<code>date</code>	Displays the current date. Example: Thu Jan 10 23:13:40 2013 GMT
<code>dnsconfig</code>	Configure DNS server parameters.
<code>dnsflush</code>	Flush DNS entries on the appliance.
<code>etherconfig</code>	Configure Ethernet port connections.
<code>externaldlpconfig</code>	Defines a minimum request body size, below which upload requests are not scanned by the external DLP server.
<code>featurekey</code>	Submits valid keys to activate licensed features.
<code>featurekeyconfig</code>	Automatically check for and update feature keys.
<code>grep</code>	Searches named input files for lines containing a match to the given pattern.

help	Returns a list of commands.
iccm_message	Clears the message in the web interface and CLI that indicates when this Web Security appliance is managed by a Security Management appliance (M-Series).
ifconfig or interfaceconfig	Configure and manage network interfaces including M1, P1, and P2. Displays currently configured interfaces, and provides an operations menu to create, edit, or delete interfaces.
last	Lists user-specific user information that includes ttys and hosts, in reverse time order or lists the users that are logged in at a specified date and time.
loadconfig	Load a system configuration file.
logconfig	Configure access to log files.
mailconfig	Mail the current configuration file to the address specified.
musconfig	Use this command to enable Secure Mobility and configure how to identify remote users, either by IP address or by integrating with one or more Cisco adaptive security appliances. Note Changes made using this command cause the Web Proxy to restart.
musstatus	Use this command to display information related to Secure Mobility when the Web Security appliance is integrated with an adaptive security appliance. This command displays the following information: <ul style="list-style-type: none"> • The status of the Web Security appliance connection with each adaptive security appliance. • The duration of the Web Security appliance connection with each adaptive security appliance in minutes. • The number of remote clients from each adaptive security appliance. • The number of remote clients being serviced, which is defined as the number of remote clients that have passed traffic through the Web Security appliance. • The total number of remote clients.
nslookup	Queries Internet domain name servers for information about specified hosts and domains or to print a list of hosts in a domain.
ntpconfig	Configure NTP servers. Displays currently configured interfaces, and provides an operations menu to add, remove, or set the interface from whose IP address NTP queries should originate.
packetcapture	Intercepts and displays TCP/IP and other packets being transmitted or received over the network to which the appliance is attached.
passwd	Set the password.
pathmtudiscovery	Enables or disables Path MTU Discovery. You might want to disable Path MTU Discovery if you need to packet fragmentation.
ping	Sends an ICMP ECHO REQUEST to the specified host or gateway.
proxyconfig <enable disable>	Enables or disables the Web Proxy.

proxystat	Display web proxy statistics.
quit, q, exit	Terminates an active process or session.
reboot	Flushes the file system cache to disk, halts all running processes, and restarts the system.
reportingconfig	Configure a reporting system.
resetconfig	Restores the configuration to factory defaults.
rollovernow	Roll over a log file.
routeconfig	Configure destination IP addresses and gateways for traffic. Displays currently configured routes, and provides an operations menu to create, edit, or delete, or clear entries.
saveconfig	Saves a copy of the current configuration settings to a file. This file can be used to restore defaults, if necessary.
setgateway	Configure the default gateway for the machine.
sethostname	Set the hostname parameter.
setntlmsecuritymode	Changes the security setting for the NTLM authentication realm to either “ads” or “domain”. <ul style="list-style-type: none"> domain — AsyncOS joins the Active Directory domain with a domain security trust account. AsyncOS requires Active Directory to use only nested Active Directory groups in this mode. ads — AsyncOS joins the domain as a native Active Directory member. Default is ads.
settime	Set system time.
settz	Displays the current time zone and the time zone version. Provides an operations menu to set a local time zone.
showconfig	Display all configuration values. Note User passwords are encrypted.
shutdown	Terminates connections and shuts down the system.
smtprelay	Configure SMTP relay hosts for internally generated email. An SMTP relay host is required to receive system generated email and alerts.
snmpconfig	Configure the local host to listen for SNMP queries and allow SNMP requests.
sshconfig	Configure hostname and host key options for trusted servers.
status	Displays system status.
supportrequest	Send the support request email to Cisco IronPort Customer Support. This includes system information and a copy of the master configuration.
tail	Displays the end of a log file. Command accepts log file name or number as parameters. example.com> tail system_logs example.com> tail 9
tcpsservices	Displays information about open TCP/IP services.

techsupport	Provides a temporary connection to allow Cisco IronPort Customer Support to access the system and assist in troubleshooting.
telnet	Communicates with another host using the TELNET protocol.
testauthconfig	<p>Tests the authentication settings for a given authentication realm against the authentication servers defined in the realm.</p> <pre>testauthconfig [-d level] [realm name]</pre> <p>Running the command without any option causes the appliance to list the configured authentication realms from which you can make a selection.</p> <p>The debug flag (-d) controls the level of debug information. The levels can range between 0-10. If unspecified, the appliance uses a level of 0. With level 0, the command will return success or failure. If the test settings fail, the command will list the cause of the failure.</p> <p>Note Cisco recommends you use level 0. Only use a different debug level when you need more detailed information to troubleshoot.</p>
traceroute	Traces IP packets through gateways and along the path to a destination host.
updateconfig	Configure update and upgrade settings.
updatenow	Update all components.
upgrade	Install an AsyncOS software upgrade.
userconfig	Configure system administrators.
version	Displays general system information, installed versions of system software, and rule definitions.
webcache	Examine or modify the contents of the proxy cache, or configure domains and URLs that the appliance never caches. Allows an administrator to remove a particular URL from the proxy cache or specify which domains or URLs to never store in the proxy cache.
who	Displays who is logged into the system.
whoami	Displays user information.



Additional Resources

- [Documentation Set, page C-1](#)
- [Training, page C-1](#)
- [Knowledge Base, page C-2](#)
- [Cisco Support Community, page C-2](#)
- [Customer Support, page C-2](#)
- [Registering for a Cisco Account to Access Resources, page C-2](#)
- [Third Party Contributors, page C-3](#)
- [Cisco Welcomes Your Comments, page C-3](#)

Documentation Set

The documentation set for Cisco content security appliances may include the following documents and books:

- *Cisco AsyncOS for Web User Guide* (this book)
- *Cisco AsyncOS CLI Reference Guide*

This and other documentation is available at the following locations:

Cisco Content Security Products Documentation:	URL
Security Management appliances	http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html
Email Security appliances and the CLI reference guide	http://www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html
Web Security appliances	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html
Cisco Encryption	http://www.cisco.com/en/US/partner/products/ps10602/tsd_products_support_series_home.html

Training

Information about security technology training:

- Web site for Cisco email and web content security training
http://www.cisco.com/web/learning/1e31/email_sec/index.html
- Email contact for information about training in Cisco security technology
stbu-trg@cisco.com
- Web site for Cisco training for Cisco products
<http://www.cisco.com/web/learning/training-index.html>

Knowledge Base

You can access the Cisco Knowledge Base on the Cisco Customer Support site at the following URL:

<http://www.cisco.com/web/ironport/knowledgebase.html>

The Knowledge Base contains how-to, troubleshooting, and reference articles related to Cisco products.

Cisco Support Community

Access the Cisco Support Community for web security and associated management at the following URL:

<https://supportforums.cisco.com/community/netpro/security/web>

The Cisco Support Community is a place to discuss general web security issues as well as technical information about specific Cisco products.

Customer Support

Use the following methods to obtain support:

U.S.: 1 (408) 526-7209 or Toll-free 1 (800) 553-2447

International: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site: http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.

Registering for a Cisco Account to Access Resources

Access to many resources on Cisco.com requires a Cisco account.

If you do not have a Cisco.com User ID, you can register for one here:

<https://tools.cisco.com/RPF/register/register.do>

Third Party Contributors

Some software included within AsyncOS is distributed under the terms, notices, and conditions of software license agreements of FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc., and other third party contributors, and all such terms and conditions are incorporated in license agreements. The full text of these agreements can be found here:

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html.

Portions of the software within AsyncOS is based upon the RRDtool with the express written consent of Tobi Oetiker.

Portions of this document are reproduced with permission of Dell Computer Corporation. Portions of this document are reproduced with permission of McAfee, Inc. Portions of this document are reproduced with permission of Sophos Plc.

Cisco Welcomes Your Comments

The Cisco Technical Publications team is interested in improving the product documentation. Your comments and suggestions are always welcome. You can send comments to the following email address: contentsecuritydocs@cisco.com

Please include the title of this book and the publication date from the title page in the subject line of your message.



End User License Agreement

- [Cisco Systems End User License Agreement, page D-1](#)
- [Supplemental End User License Agreement for Cisco Systems Content Security Software, page D-8](#)

Cisco Systems End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN APPROVED SOURCE, AND APPLIES ONLY IF YOU ARE THE ORIGINAL AND REGISTERED END USER PURCHASER. FOR THE PURPOSES OF THIS END USER LICENSE AGREEMENT, AN "APPROVED SOURCE" MEANS (A) CISCO; OR (B) A DISTRIBUTOR OR SYSTEMS INTEGRATOR AUTHORIZED BY CISCO TO DISTRIBUTE /

SELL CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS; OR (C) A RESELLER AUTHORIZED BY ANY SUCH DISTRIBUTOR OR SYSTEMS INTEGRATOR IN ACCORDANCE WITH THE TERMS OF THE DISTRIBUTOR'S AGREEMENT WITH CISCO TO DISTRIBUTE / SELL THE CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS.

THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER'S USE OF THE SOFTWARE (DEFINED BELOW), EXCEPT TO THE EXTENT: (A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND CISCO GOVERNING CUSTOMER'S USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE "CLICK-ACCEPT" LICENSE AGREEMENT OR THIRD PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION OR DOWNLOAD PROCESS GOVERNING CUSTOMER'S USE OF THE SOFTWARE. TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE (1) THE SIGNED CONTRACT, (2) THE CLICK-ACCEPT AGREEMENT OR THIRD PARTY LICENSE AGREEMENT, AND (3) THE AGREEMENT. FOR PURPOSES OF THE AGREEMENT, "SOFTWARE" SHALL MEAN COMPUTER PROGRAMS, INCLUDING FIRMWARE AND COMPUTER PROGRAMS EMBEDDED IN CISCO EQUIPMENT, AS PROVIDED TO CUSTOMER BY AN APPROVED SOURCE, AND ANY UPGRADES, UPDATES, BUG FIXES OR MODIFIED VERSIONS THERETO (COLLECTIVELY, "UPGRADES"), ANY OF THE SAME WHICH HAS BEEN RELICENSED UNDER THE CISCO SOFTWARE TRANSFER AND RE-LICENSING POLICY (AS MAY BE AMENDED BY CISCO FROM TIME TO TIME) OR BACKUP COPIES OF ANY OF THE FOREGOING.

License. Conditioned upon compliance with the terms and conditions of the Agreement, Cisco grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees to an Approved Source. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by an Approved Source with the Software in any manner (including on CD-Rom, or on-line). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of the Software online at Cisco's website to obtain the necessary license key or license file.

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement or in the applicable purchase order which has been accepted by an Approved Source and for which Customer has paid to an Approved Source the required license fee (the "Purchase Order").

Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customer's internal business purposes. No other licenses are granted by implication, estoppel or otherwise.

For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Cisco or its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Except as otherwise expressly provided under the Agreement, Customer shall only use the Software in connection with the use of Cisco equipment purchased by the Customer from an Approved Source and Customer shall have no right, and Customer specifically agrees not to:

- (i) transfer, assign or sublicense its license rights to any other person or entity (other than in compliance with any Cisco relicensing/transfer policy then in force), or use the Software on Cisco equipment not purchased by the Customer from an Approved Source or on secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;
- (ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;
- (iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction or except to the extent that Cisco is legally required to permit such specific activity pursuant to any applicable open source license;
- (iv) publish any results of benchmark tests run on the Software;
- (v) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or
- (vi) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by applicable law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available.

Software, Upgrades and Additional Copies. NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO MAKE OR USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF MAKING OR ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE TO AN APPROVED SOURCE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT SUPPLIED BY AN APPROVED SOURCE FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright, proprietary, and other notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in the Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

Term and Termination. The Agreement and the license granted herein shall remain effective until terminated. Customer may terminate the Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under the Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of the Agreement. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer, all restrictions and limitations imposed on the Customer under the section titled "General Limitations" and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License Agreement" shall survive termination of the Agreement.

Customer Records. Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

Export, Re-Export, Transfer and Use Controls. The Software, Documentation and technology or direct products thereof (hereafter referred to as Software and Technology), supplied by Cisco under the Agreement are subject to export controls under the laws and regulations of the United States (U.S.) and any other applicable countries' laws and regulations. Customer shall comply with such laws and regulations governing export, re-export, transfer and use of Cisco Software and Technology and will obtain all required U.S. and local authorizations, permits, or licenses. Cisco and Customer each agree to provide the other information, support documents, and assistance as may reasonably be required by the other in connection with securing authorizations or licenses. Information regarding compliance with export, re-export, transfer and use may be located at the following URL:

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which the Agreement may be incorporated, Customer may provide to Government end user or, if the Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in the Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Identified Components; Additional Terms. The Software may contain or be delivered with one or more components, which may include third-party components, identified by Cisco in the Documentation, readme.txt file, third-party click-accept or elsewhere (e.g. on www.cisco.com) (the "Identified Component(s)") as being subject to different license agreement terms, disclaimers of warranties, limited warranties or other terms and conditions (collectively, "Additional Terms") than those set forth herein. You agree to the applicable Additional Terms for any such Identified Component(s)."

Limited Warranty

Subject to the limitations and conditions set forth herein, Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an Approved Source other than Cisco, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided "AS IS". This limited warranty extends only to the Software purchased from an Approved Source by a Customer who is the first registered end user. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers under this limited warranty will be (i) replacement of defective media and/or (ii) at Cisco's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to the Approved Source supplying the Software to Customer, within the warranty period. Cisco or the Approved Source supplying the Software to Customer may, at its option, require return of the Software and/or Documentation as a condition to the remedy. In no event does Cisco warrant that the Software is

error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing or demonstration purposes. The Software warranty also does not apply to (e) any temporary Software modules; (f) any Software not posted on Cisco's Software Center; (g) any Software that Cisco expressly provides on an "AS IS" basis on Cisco's Software Center; (h) any Software for which an Approved Source does not receive a license fee; and (i) Software supplied by any third party which is not an Approved Source.

DISCLAIMER OF WARRANTY

EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT THAT ANY OF THE SAME CANNOT BE EXCLUDED, SUCH IMPLIED CONDITION, REPRESENTATION AND/OR WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD REFERRED TO IN THE "LIMITED WARRANTY" SECTION ABOVE. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY IN SUCH STATES. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

Disclaimer of Liabilities - Limitation of Liability. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, CANADA, JAPAN OR THE CARIBBEAN, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO ANY APPROVED SOURCE FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT).

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO CISCO FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID

FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT). NOTHING IN THE AGREEMENT SHALL LIMIT (I) THE LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS TO CUSTOMER FOR PERSONAL INJURY OR DEATH CAUSED BY THEIR NEGLIGENCE, (II) CISCO'S LIABILITY FOR FRAUDULENT MISREPRESENTATION, OR (III) ANY LIABILITY OF CISCO WHICH CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Disclaimer of Liabilities - Waiver of Consequential Damages and Other Losses. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, THE CARIBBEAN OR CANADA, REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

IF YOU ACQUIRED THE SOFTWARE IN JAPAN, EXCEPT FOR LIABILITY ARISING OUT OF OR IN CONNECTION WITH DEATH OR PERSONAL INJURY, FRAUDULENT MISREPRESENTATION, AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ANY APPROVED SOURCE OR THEIR SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, BE LIABLE FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, HOWSOEVER ARISING, INCLUDING, WITHOUT LIMITATION, IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF, IN EACH CASE, CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT FULLY APPLY TO YOU. THE FOREGOING EXCLUSION SHALL NOT APPLY TO ANY LIABILITY ARISING OUT OF OR IN CONNECTION WITH: (I) DEATH OR PERSONAL INJURY, (II) FRAUDULENT MISREPRESENTATION, OR (III) CISCO'S LIABILITY IN CONNECTION WITH ANY TERMS THAT CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Customer acknowledges and agrees that Cisco has set its prices and entered into the Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

Controlling Law, Jurisdiction. If you acquired, by reference to the address on the purchase order accepted by the Approved Source, the Software in the United States, Latin America, or the Caribbean, the Agreement and warranties ("Warranties") are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Canada, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the Province of Ontario, Canada, notwithstanding any conflicts of law provisions; and the courts of the Province of Ontario shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Europe, the Middle East, Africa, Asia or Oceania (excluding Australia), unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of England, notwithstanding any conflicts of law provisions; and the English courts shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. In addition, if the Agreement is controlled by the laws of England, no person who is not a party to the Agreement shall be entitled to enforce or take the benefit of any of its terms under the Contracts (Rights of Third Parties) Act 1999. If you acquired the Software in Japan, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of Japan, notwithstanding any conflicts of law provisions; and the Tokyo District Court of Japan shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Australia, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of New South Wales, Australia, notwithstanding any conflicts of law provisions; and the State and federal courts of New South Wales shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in any other country, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.

For all countries referred to above, the parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement and Warranties shall remain in full force and effect. Except as expressly provided herein, the Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any Purchase Order or elsewhere, all of which terms are excluded. The Agreement has been written in the English language, and the parties agree that the English version will govern.

Product warranty terms and other information applicable to Cisco products are available at the following URL:

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

Supplemental End User License Agreement for Cisco Systems Content Security Software

IMPORTANT: READ CAREFULLY

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software product licensed under the End User License Agreement ("EULA") between You ("You" as used herein means You and the business entity you represent or "Company") and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA.

DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

For purposes of this SEULA, the Product name and the Product description You have ordered is any of the following Cisco Systems Email Security Appliance ("ESA"), Cisco Systems Web Security Appliance ("WSA") and Cisco Systems Security Management Application ("SMA") (collectively, "Content Security") and their Virtual Appliance equivalent ("Software"):

- Cisco AsyncOS for Email
- Cisco AsyncOS for Web
- Cisco AsyncOS for Management
- Cisco Email Anti-Spam, Sophos Anti-Virus
- Cisco Email Outbreak Filters
- Cloudmark Anti-Spam
- Cisco Image Analyzer
- McAfee Anti-Virus
- Cisco Intelligent Multi-Scan
- Cisco RSA Data Loss Prevention
- Cisco Email Encryption
- Cisco Email Delivery Mode
- Cisco Web Usage Controls
- Cisco Web Reputation
- Sophos Anti-Malware
- Webroot Anti-Malware

McAfee Anti-Malware
Cisco Email Reporting
Cisco Email Message Tracking
Cisco Email Centralized Quarantine
Cisco Web Reporting
Cisco Web Policy and Configuration Management
Cisco Advanced Web Security Management with Splunk
Email Encryption for Encryption Appliances
Email Encryption for System Generated Bulk Email
Email Encryption and Public Key Encryption for Encryption Appliances
Large Attachment Handling for Encryption Appliances
Secure Mailbox License for Encryption Appliances

Definitions

For purposes of this SEULA, the following definitions apply:

"Company Service" means the Company's email, Internet, security management services provided to End Users for the purposes of conducting Company's internal business.

"End User" means: (1) for the WSA and SMA, the employee, contractor or other agent authorized by Company to access the Internet and the SMA via the Company Service; and (2) for the ESA, the email boxes of the employees, contractors, or other agent authorized by Company to access or use the email services via the Company Service.

"Ordering Document" means the purchase agreement, evaluation agreement, beta, pre-release agreement or similar agreement between the Company and Cisco or the Company and a Cisco reseller, or the valid terms of any purchase order accepted by Cisco in connection therewith, containing the purchase terms for the Software license granted by this Agreement.

"Personally Identifiable Information" means any information that can be used to identify an individual, including, but not limited to, an individual's name, user name, email address and any other personally identifiable information.

"Server" means a single physical computer or devices on a network that manages or provides network resources for multiple users.

"Services" means Cisco Software Subscription Services.

"Service Description" means the description of the Software Subscription Support Services at http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html

"Telemetry Data" means samples of Company's email and web traffic, including data on email message and web request attributes and information on how different types of email messages and web requests were handled by Company's Cisco hardware products. Email message metadata and web requests included in Telemetry Data are anonymized and obfuscated to remove any Personally Identifiable Information.

"Term" means the length of the Software subscription You purchased, as indicated in your Ordering Document.

"Virtual Appliance" means the virtual version of Cisco's email security appliances, web security appliances, and security management appliances.

"Virtual Machine" means a software container that can run its own operating system and execute applications like a Server.

Additional License Terms and Conditions

LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

License of Software.

By using the Software and the Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, Cisco hereby grants to Company a nonexclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on Cisco's hardware products, or in the case of the Virtual Appliances, on a Virtual Machine, solely in connection with the provision of the Company Service to End Users. The number of End Users licensed for the use of the Software is limited to the number of End Users specified in the Ordering Documents. In the event that the number of End Users in connection with the provision of the Company Service exceeds the number of End Users specified in the Ordering Documents, Company shall contact an Approved Source to purchase additional licenses for the Software. The duration and scope of this license(s) is further defined in the Ordering Document. The Ordering Document supersedes the EULA with respect to the term of the Software license. Except for the license rights granted herein, no right, title or interest in any Software is granted to the Company by Cisco, Cisco's resellers or their respective licensors. Your entitlement to Upgrades to the Software is subject to the Service Description. This Agreement and the Services are co-terminus.

Consent and License to Use Data.

Subject to the Cisco Privacy Statement at <http://www.cisco.com/web/siteassets/legal/privacy.html>, Company hereby consents and grants to Cisco a license to collect and use Telemetry Data from the Company. Cisco does not collect or use Personally Identifiable Information in the Telemetry Data. Cisco may share aggregated and anonymous Telemetry Data with third parties to assist us in improving your user experience and the Software and other Cisco security products and services. Company may terminate Cisco's right to collect Telemetry Data at any time by disabling SenderBase Network Participation in the Software. Instructions to enable or disable SenderBase Network Participation are available in the Software configuration guide.

Description of Other Rights and Obligations

Please refer to the Cisco Systems, Inc. End User License Agreement, Privacy Statement and Service Description of Software Subscription Support Services.



A

access log file

see also *W3C access logs*

ACL decision tags [20-33](#)

overview [20-12](#)

result codes [20-32](#)

URL category abbreviations [9-22](#)

access logs

header format specifier [20-31](#)

Access Policies [9-5](#)

and URL category changes [9-5](#)

configuring Web Reputation [13-12](#)

proxy port of request [5-18](#)

subnet of request [5-18](#)

time of request [5-18](#)

URL filters [10-10](#)

ACL decision tags

access log file [20-33](#)

Active Directory [6-1](#)

adding

log subscriptions [20-5](#)

WCCP service [3-21](#)

addresses

ambiguous address [19-2](#)

known allowed address [19-2](#)

known malware address [19-2](#)

adminaccessconfig command

overview [21-12](#)

adult content

filtering [9-15](#)

logging usage [9-16](#)

alert listing [21-15](#)

alerts

alert classifications [21-13](#)

severities [21-13](#)

alert types [21-13](#)

ambiguous address

defined [19-2](#)

AMW

see *anti-malware*

anonymizing

usernames in reports [17-1](#)

anti-malware

access log file [13-13](#)

configuring [13-8](#)

database [13-13](#)

outbound scanning [12-1](#)

overview [13-4](#)

rules for L4 Traffic Monitor [19-2](#)

scanning verdicts [20-36](#)

Anti-Malware report [18-5](#)

anti-malware rules

L4 Traffic Monitor [19-2](#)

anti-malware scanning

outbound [12-1](#)

application behaviors

defined [14-2](#)

application control

application behaviors [14-2](#)

applications [14-2](#)

application types [14-2](#)

bandwidth [14-4](#)

configuring [14-2, 14-4](#)

instant messaging traffic [14-6](#)

logging [14-7](#)

- overview [14-1](#)
- report [18-4](#)
- reporting [14-7](#)
- applications
 - blocking [14-4](#)
 - configuring bandwidth limits [14-6](#)
 - defined [14-2](#)
- application types
 - configuring bandwidth limits [14-5](#)
 - defined [14-2](#)
 - overriding bandwidth limits [14-6](#)
- Application Visibility report
 - overview [18-4](#)
- archiving reports [17-10](#)
- AsyncOS reversion [21-32](#)
- authentication credentials
 - SaaS Access Control [8-2](#)
- available upgrades [21-27](#)
- AVC engine
 - enabling [14-3](#)
 - updates [14-3](#)

B

- bandwidth
 - configuring overall limits [14-5](#)
 - configuring user limits [14-5](#)
 - limiting [14-4](#)
- bandwidth limits
 - configuring for applications [14-6](#)
 - configuring for application types [14-5](#)
 - overall [14-5](#)
 - overriding for application types [14-6](#)
 - overview [14-4](#)
 - per user [14-5](#)
- blacklist address
 - see *known malware address*
- blocking
 - adult content [9-15](#)

- all traffic by default [3-13](#)
- applications [14-4](#)
- HTTPS traffic [11-9](#)
- objects [15-8](#)
- upload requests [15-2](#)
- upload requests due to AVC engine [14-3](#)
- upload requests due to malware [12-1](#)
- URL categories [15-8](#)
- user experience [12-1, 14-3, 15-2](#)
- blocking traffic
 - by default in System Setup Wizard [3-13](#)
- block objects [10-8](#)
- browsers
 - see *web browsers*
- bypassing
 - decryption [A-5](#)
 - upload requests from scanning [15-2](#)

C

- caching [13-14](#)
- capturing network packets
 - overview [21-4](#)
- case-sensitivity
 - in CLI [B-3](#)
- categories
 - adult [9-23](#)
 - advertisements [9-23](#)
 - alcohol [9-23](#)
 - arts [9-23](#)
 - astrology [9-23](#)
 - auctions [9-23](#)
 - business and industry [9-23](#)
 - chat and instant messaging [9-23](#)
 - cheating and plagiarism [9-24](#)
 - child abuse content [9-24](#)
 - computers and internet [9-24](#)
 - computer security [9-24](#)
 - dating [9-24](#)

- digital postcards [9-24](#)
- dining and drinking [9-24](#)
- dynamic and residential [9-24](#)
- education [9-24](#)
- entertainment [9-24](#)
- extreme [9-24](#)
- fashion [9-24](#)
- file transfer services [9-25](#)
- filter avoidance [9-25](#)
- finance [9-25](#)
- freeware and shareware [9-25](#)
- gambling [9-25](#)
- games [9-25](#)
- government and law [9-25](#)
- hacking [9-25](#)
- hate speech [9-25](#)
- health and nutrition [9-26](#)
- humor [9-26](#)
- illegal activities [9-26](#)
- illegal downloads [9-26](#)
- illegal drugs [9-26](#)
- infrastructure and content delivery networks [9-26](#)
- internet telephony [9-26](#)
- job search [9-26](#)
- lingerie and swimsuits [9-26](#)
- lotteries [9-26](#)
- mobile phones [9-26](#)
- nature [9-27](#)
- news [9-27](#)
- non-governmental organizations [9-27](#)
- non-sexual nudity [9-27](#)
- online communities [9-27](#)
- online storage and backup [9-27](#)
- online trading [9-27](#)
- organizational email [9-27](#)
- parked domains [9-27](#)
- peer file transfer [9-27](#)
- personal sites [9-27](#)
- photo searches and images [9-28](#)
- politics [9-28](#)
- pornography [9-28](#)
- professional networking [9-28](#)
- real estate [9-28](#)
- reference [9-28](#)
- religion [9-28](#)
- SaaS and B2B [9-28](#)
- safe for kids [9-28](#)
- science and technology [9-28](#)
- search engines and portals [9-28](#)
- sex education [9-28](#)
- shopping [9-28](#)
- social networking [9-28](#)
- social science [9-29](#)
- society and culture [9-29](#)
- software updates [9-29](#)
- sports and recreation [9-29](#)
- streaming audio [9-29](#)
- streaming video [9-29](#)
- tobacco [9-29](#)
- transportation [9-29](#)
- travel [9-29](#)
- unclassified [9-29](#)
- weapons [9-29](#)
- web-based email [9-30](#)
- web hosting [9-29](#)
- web page translation [9-30](#)
- category filtering
 - database [9-3](#)
- certificate files
 - supported formats [11-5](#)
 - uploading [11-7](#)
- certificates
 - CSR for HTTPS Proxy [11-8](#)
 - CSR for Identity Provider for SaaS [8-3](#)
 - CSR for web interface [21-24](#)
 - FIPS [21-21](#)
 - generating and signing your own [21-24](#)
 - installing on appliance [21-24](#)

- invalid [11-8, 11-9](#)
- SaaS Access Control [8-2](#)
- validating [11-6](#)
- Certificate Signing Request (CSR)
 - for HTTPS Proxy [11-8](#)
 - for Identity Provider for SaaS [8-3](#)
 - for web interface [21-24](#)
- Change Password link [21-9](#)
- changing passwords [21-9](#)
- Cisco ASA integration
 - overview [10-18](#)
- Cisco Cloud Web Security
 - guest users [4-11](#)
- Cisco Data Security Policies
 - and URL category changes [9-5](#)
- Cisco IronPort Data Security Policies
 - see *Data Security Policies*
 - user location of request [15-7](#)
- Cisco Web Usage Controls
 - overview [9-1](#)
- CLI
 - case-sensitivity in [B-3](#)
 - configuring host keys [20-10](#)
 - configuring languages [21-11](#)
 - overview [B-1](#)
 - SSH [B-1](#)
- Client Malware Risk [18-6](#)
- Client Malware Risk report [18-6](#)
- Client Malware Risk report page [18-6](#)
- Client Signing Required [6-5, 6-7](#)
- Cloud Connector
 - authentication failures [4-11](#)
- Cloud Web Security Connector [1-1](#)
 - FTP [4-9](#)
 - changing modes [4-11](#)
 - cloud connector settings [4-6](#)
 - cloud routing policies [4-9](#)
 - Cloud Web Security Connector
 - HTTPS [4-9](#)
 - compared to standard mode [4-2](#)
 - Configuring [4-5](#)
 - data loss prevention [4-10](#)
 - directory group policies [4-8](#)
 - documentation [4-4](#)
 - logging [4-10](#)
 - Overview [4-1](#)
 - setting the appliance mode [4-6](#)
 - user authentication [4-11](#)
- commit command [B-4](#)
- community string
 - SNMP [17-11](#)
- configuring [3-19](#)
 - administrator settings [21-12](#)
 - application control settings [14-2](#)
 - HTTPS Proxy [11-3](#)
 - return addresses [21-13](#)
 - URL filters [9-9](#)
 - Web Reputation Filters [13-12](#)
- configuring the appliance
 - anti-malware [13-8](#)
 - browser requirements [1-3](#)
 - enabling features [21-6](#)
 - network interfaces [3-16](#)
 - reporting [17-1](#)
 - scheduling reports [17-8](#)
- content filtering
 - Cisco IronPort Data Security Policies [15-8](#)
- controlling applications
 - overview [14-1](#)
- controlling bandwidth
 - overall limits [14-5](#)
 - overview [14-4](#)
 - user limits [14-5](#)
- control settings
 - Decryption Policies [11-4](#)
- creating

- Cisco IronPort Data Security Policies [15-5](#)
- External DLP Policies [15-5](#)
- log subscriptions [20-5](#)
- Outbound Malware Scanning Policies [12-3](#)
- CSS
 - in end-user notification pages [16-13](#)
- custom
 - date ranges [17-2](#)
 - end-user notification pages [16-5](#)
 - headers [20-31](#)
 - URL categories [9-13](#)
 - redirecting traffic [9-17](#)
- custom mask for load balancing [3-23](#)

D

- data loss prevention
 - see *Outbound Malware Scanning Policies*
- Data Loss Prevention Policies, External [9-5](#)
- `datasecurityconfig`
 - CLI command [15-2](#)
- Data Security logs
 - overview [15-11](#)
- Data Security Policies
 - configuring [15-7](#)
 - content [15-8](#)
 - creating [15-5](#)
 - flow diagram [15-8](#)
 - logging [15-11](#)
 - membership [15-4](#)
 - minimum request size [15-2](#)
 - protocol of request [15-6](#)
 - proxy port of request [15-6](#)
 - subnet of request [15-6](#)
 - URL category of request [15-6](#)
 - URL filters [15-8](#)
 - user agent of request [15-7](#)
 - Web Reputation [15-8](#)
- Data Security Policies, Cisco [9-5](#)

- decrypting
 - HTTPS traffic [11-2](#)
- decrypting HTTPS traffic
 - configuring Decryption Policies [11-1](#)
- decryption
 - bypassing [A-5](#)
- Decryption Policies [9-5](#)
 - and URL category changes [9-5](#)
 - blocking [11-9](#)
 - bypassing decryption [A-5](#)
 - controlling traffic [11-4](#)
 - control settings [11-4](#)
 - decrypting traffic [11-1](#)
 - dropping traffic [11-1](#)
 - enabling [11-3](#)
 - logging [A-6](#)
 - Monitor action [11-2](#)
 - overview [11-2](#)
 - passing through traffic [11-1](#)
- Decryption Policy groups
 - see also *policy groups*
- default gateway [3-19](#)
- default identity [7-1](#)
- default route
 - configuring [3-19](#)
- defining
 - user preferences [21-11](#)
- deleting
 - log subscriptions [20-8](#)
- DLP servers
 - defining [15-9](#)
 - failover [15-10](#)
- DNS
 - authoritative name servers [3-31](#)
 - configuring [3-31](#)
 - split [3-31](#)
- DNS cache
 - flushing [3-32](#)
- dropping traffic

Decryption Policies [11-1](#)

DVS engine

- how it works [13-4](#)
- working with multiple malware verdicts [13-5](#)

Dynamic Content Analysis engine

- enabling [9-4](#)

Dynamic Vectoring and Streaming engine

- see *DVS engine*

E

editing

- WCCP service [3-21](#)

editing the appliance

- concurrent editing [1-3](#)

enabling

- HTTPS Proxy [11-3](#)

end-user acknowledgement page

- configuring [16-11](#)
- FTP requests [16-12](#)
- HTTPS requests [16-12](#)
- overview [16-10](#)

end-user notification pages

- customizing [16-5](#)
- formatting text [16-13](#)
- HTML tags [16-13](#)
- native FTP [16-13](#)
- on-box notification pages [16-4](#)
- tokens [16-5](#)
- user defined notification pages [16-8](#)
- variables [16-5](#)

end-user URL category page

- configuring [16-12](#)
- warning users [9-17](#)

etherconfig command

- VLAN [3-25](#)

evaluating Data Security Policy membership

- matching client requests [15-4](#)

evaluating External DLP Policy membership

- matching client requests [15-4](#)

evaluating Outbound Malware Scanning membership

- matching client requests [12-2](#)

expired keys

- overview [A-4](#)

exporting

- reports [17-7](#)

External Data Loss Prevention

- and URL Category changes [9-5](#)

externaldlpconfig

- CLI command [15-2](#)

External DLP Policies

- configuring [15-11](#)
- creating [15-5](#)
- defining external DLP servers [15-9](#)
- load balancing [15-10](#)
- logging [15-11](#)
- membership [15-4](#)
- minimum request size [15-2](#)
- protocol of request [15-6](#)
- proxy port of request [15-6](#)
- subnet of request [15-6](#)
- URL category of request [15-6](#)
- user agent of request [15-7](#)
- user location of request [15-7](#)

external DLP servers

- see *DLP servers*

F

failover

- DLP servers [15-10](#)

feature keys

- adding manually [21-6](#)
- expired keys [A-4](#)
- overview [21-6](#)
- settings [21-6](#)

Federal Information Processing Standards [21-20](#)

Federal Information Processing Standards (FIPS) [21-20](#)

filtering

- adult content [9-15](#)
- category [10-10, 15-8](#)
- data in Cisco IronPort Data Security Policies [15-8](#)
- Web Reputation [15-8](#)

FIPS

- certificate requirements [21-21](#)
- compliance [21-20](#)
- mode [21-21](#)

formatting

- end-user acknowledge pages [16-13](#)
- end-user notification pages [16-13](#)

forwarding method

- L2 [3-23](#)

FTP

- configuring notification messages [16-13](#)
- end-user acknowledgement page [16-12](#)

G

generating

- root certificates [11-3](#)

global identity [7-1](#)

greylist address

- see *ambiguous address*

GUI

- configuring language [21-11](#)

Hhash versus mask for load balancing [3-23](#)

headers

- custom [20-31](#)

heuristic analysis

- McAfee scanning engine [13-6](#)

hostkeyconfig command [20-10](#)

hostname

- changing [3-30](#)

HTTPS

- bypassing decryption [A-5](#)
- end-user acknowledgement page [16-12](#)
- logging [A-6](#)
- routing [11-10](#)

HTTPS Proxy

- configuring [11-3](#)
- Ports to Proxy [11-3](#)

I
Identities [9-5](#)

- and URL category changes [9-5](#)

installation

- reverting [21-32](#)

installing the appliance

- setup worksheet [3-5](#)

instant messaging traffic

- controlling [14-6](#)

interfaceconfig command

- VLAN [3-27](#)

invalid

- signing, leaf certificate [11-9](#)

invalid certificates

- handling [11-9](#)

IPMI

- SNMP [17-12](#)

IP spoofing

- WCCP service [3-24](#)

IPv4 [3-17](#)IPv4/IPv6 [3-15](#)IPv6 [3-17](#)

KKerberos [6-1](#)

key files

- supported formats [11-5](#)

- keys
 - overview [21-6](#)
- known allowed address
 - defined [19-2](#)
- known malware address
 - defined [19-2](#)

L

- L2
 - forwarding method [3-23](#)
- L4 Traffic Monitor
 - ambiguous addresses [19-2](#)
 - anti-malware rules [19-2](#)
 - interfaces [3-4](#)
 - known allowed addresses [19-2](#)
 - known malware addresses [19-2](#)
 - log files [20-18](#)
 - report [18-7](#)
 - viewing activity [19-4](#)
- L4 Traffic Monitor interfaces
 - overview [3-4](#)
- languages
 - defining default per user [21-11](#)
 - user preferences [21-11](#)
- LDAP [6-1](#)
- load balancing
 - traffic to external DLP servers [15-10](#)
- load-balancing method [3-23](#)
- loadlicense [21-7](#)
- log files
 - L4 Traffic Monitor [20-18](#)
 - naming convention [20-3](#)
 - types [20-19](#)
 - viewing most recent version [20-9](#)
- logging
 - HTTPS requests [A-6](#)
 - redirected traffic [9-17](#)
 - SMTP transactions [20-20](#)

- YouTube headers [20-31](#)
- log subscriptions
 - adding [20-5](#)
 - deleting [20-8](#)
 - editing [20-5](#)

M

- MAIL FROM
 - configuring for notifications [21-13](#)
- malware
 - configuring scanning [13-8](#)
 - see also *anti-malware*
- malware verdicts
 - multiple [13-5](#)
- mask customization for load balancing [3-23](#)
- mask versus hash for load balancing [3-23](#)
- matching client requests
 - Cisco IronPort Data Security Policies [15-4](#)
 - External DLP Policies [15-4](#)
 - Outbound Malware Scanning Policies [12-2](#)
- McAfee scanning engine
 - categories [13-7](#)
 - database [13-13](#)
 - heuristic analysis [13-6](#)
 - overview [13-6](#)
- membership diagram
 - Cisco IronPort Data Security Policies [15-4](#)
 - External DLP Policies [15-4](#)
 - Outbound Malware Scanning Policies [12-2](#)
- MIB file
 - SNMP [17-11](#)
- misclassified URLs
 - reporting [16-5](#)
 - URL submission tool [9-3](#)
- Monitor
 - Decryption Policies [11-2](#)
- monitoring
 - scheduling reports [17-8](#)

- summary data [17-1](#)
- system activity [18-1](#)

N

- native FTP
 - configuring notification messages [16-13](#)
 - with transparent redirection and IP spoofing [3-22](#)
- navigating
 - web interface [1-3](#)
- network interfaces [3-16](#)
 - T1 and T2 [3-4](#)
- NTLMSSP [6-1](#)

O

- object blocking [10-8](#)
- objects
 - blocking [15-8](#)
- OCSP [11-9](#)
- on-box notification pages
 - overview [16-4](#)
- outbound malware scanning
 - overview [12-1](#)
- Outbound Malware Scanning Policies [9-5](#)
 - configuring [12-4](#)
 - creating [12-3](#)
 - logging [12-6](#)
 - membership [12-2](#)
 - protocol of request [12-3](#)
 - proxy port of request [12-3](#)
 - subnet of request [12-4](#)
 - URL category of request [12-4](#)
 - user agent of request [12-4](#)
 - user location of request [12-4](#)
- Outbound Malware Scan Policy
 - and URL category changes [9-5](#)
- Overview report [18-1](#)

P

- packet capture
 - overview [21-4](#)
 - starting [21-4](#)
- passing through traffic
 - Decryption Policies [11-1](#)
- passwords
 - changing [21-9](#)
- PDF
 - reports [17-7](#)
- policy group member definition
 - Cisco IronPort Data Security Policies [15-4](#)
 - External DLP Policies [15-4](#)
 - Outbound Malware Scanning Policies [12-2](#)
- policy groups
 - custom URL categories [9-13](#)
 - Decryption Policies [11-1](#)
- ports
 - Access Policies [5-18](#)
 - Cisco IronPort Data Security Policies [15-6](#)
 - External DLP Policies [15-6](#)
 - Outbound Malware Scanning Policies [12-3](#)
- Ports to Proxy
 - HTTPS [11-3](#)
- preferences
 - defining for users [21-11](#)
- protocols
 - Cisco IronPort Data Security Policies [15-6](#)
 - External DLP Policies [15-6](#)
 - Outbound Malware Scanning Policies [12-3](#)
- proxy
 - see *web proxy*
- Proxy Buffer Memory [18-12](#)

R

- redirecting traffic
 - logging and reporting [9-17](#)

- regular expressions
 - overview [9-20](#)
 - using in URL filters [9-20](#)
 - remote upgrades [21-29, 21-30](#)
 - reporting
 - redirected traffic [9-17](#)
 - reporting misclassified URLs [16-5](#)
 - reports
 - anonymizing usernames [17-1](#)
 - Anti-Malware [18-5](#)
 - Application Visibility [18-4](#)
 - archiving [17-10](#)
 - charts [17-4](#)
 - Client Detail [18-6](#)
 - Client Malware Risk [18-6](#)
 - Client Malware Risk Page [18-6](#)
 - custom date ranges [17-2](#)
 - exporting data [17-7](#)
 - graphs [17-4](#)
 - interactive display [17-1](#)
 - L4 Traffic Monitor [18-7](#)
 - making usernames unrecognizable [17-1](#)
 - Malware Category [18-5](#)
 - Malware Threat [18-5](#)
 - Overview [18-1](#)
 - printing to PDF [17-7](#)
 - Reports by User Location [18-8](#)
 - return address [21-13](#)
 - scheduling [17-8](#)
 - search option [17-3](#)
 - System Capacity [18-11](#)
 - System Status [18-12](#)
 - time range for scheduled reports [17-8](#)
 - time ranges [17-2](#)
 - uncategorized URLs [18-4](#)
 - URL Categories [18-3](#)
 - Web Reputation Filters [18-6](#)
 - Web Sites [18-3](#)
 - Reports by User Location report
 - overview [18-8](#)
 - result codes [20-32](#)
 - return addresses
 - configuring [21-13](#)
 - revert
 - installation [21-32](#)
 - RFC
 - 1065 [17-11](#)
 - 1066 [17-11](#)
 - 1067 [17-11](#)
 - 1213 [17-11](#)
 - 1907 [17-11](#)
 - 2571-2575 [17-11](#)
 - rolling over log files [20-4](#)
 - root certificates
 - generating [11-3](#)
 - uploading [11-3](#)
 - routes
 - default route [3-19](#)
 - overview [3-18](#)
 - split routing [3-19](#)
 - routing
 - HTTPS [11-10](#)
 - Routing Policies [9-5](#)
 - and URL category changes [9-5](#)
-
- S**
- SaaS Access Control
 - authenticating users [8-2](#)
 - certificate [8-2](#)
 - multiple appliances [8-4](#)
 - overview [8-1](#)
 - prompting for authentication [8-2](#)
 - zero day revocation [8-1](#)
 - safe search
 - enforcing [9-15](#)
 - scanning verdicts
 - anti-malware [20-36](#)

- Secure Mobility
 - report [18-8](#)
 - SensorBase Network [1-4](#)
 - sethostname command
 - overview [3-30](#)
 - Simple Network Management Protocol
 - see *SNMP*
 - site content rating
 - enforcing [9-15](#)
 - SMI file
 - SNMP [17-11](#)
 - SMTP transactions
 - logging [20-20](#)
 - SNMP
 - community string [17-11](#)
 - hardware objects [17-12](#)
 - IPMI [17-12](#)
 - MIB file [17-11](#)
 - overview [17-11](#)
 - SMI file [17-11](#)
 - SNMPv1 [17-11](#)
 - SNMPv2 [17-11](#)
 - SNMPv3 passphrase [17-11](#)
 - specifying multiple trap targets [17-12](#)
 - traps [17-12](#)
 - SOCKS
 - configuring [5-17](#)
 - enabling [5-16](#)
 - overview [5-16](#)
 - policies [5-17](#)
 - Sophos scanning engine
 - overview [13-7](#)
 - split routing
 - defined [3-19](#)
 - SSH
 - using with the CLI [B-1](#)
 - subnet
 - Access Policies [5-18](#)
 - Cisco IronPort Data Security Policies [15-6](#)
 - External DLP Policies [15-6](#)
 - Outbound Malware Scanning Policies [12-4](#)
 - supported languages
 - configuring default [21-11](#)
 - supportrequest command [21-3](#)
 - System Capacity report
 - overview [18-11](#)
 - System Setup Wizard
 - Security page [3-13](#)
 - System Status report [18-12](#)
-
- T**
- T1 and T2 interfaces
 - overview [3-4](#)
 - Threat Risk Threshold
 - Webroot [13-8](#)
 - time based policies
 - URL Filters [9-19](#)
 - time ranges
 - Access Policies [5-18](#)
 - tokens
 - see *variables*
 - transaction result codes [20-32](#)
 - transparent mode
 - transparent redirection [3-20](#)
 - transparent redirection [3-23](#)
 - adding a WCCP service [3-21](#)
 - L2 forwarding method [3-23](#)
 - overview [3-20](#)
 - WCCP services [3-21](#)
-
- U**
- UDP_MISS [20-32](#)
 - uncategorized URLs
 - defined [9-2](#)
 - in reports [18-4](#)

- URL submission tool [9-3](#)
 - unrecognized
 - root authority/issuer [11-9](#)
 - unrecognized root authority
 - invalid certificates [11-9](#)
 - updates
 - manual updates [21-27](#)
 - overview [21-31](#)
 - upgrades
 - available [21-27](#)
 - configuring upgrade settings [21-31](#)
 - remote [21-29, 21-30](#)
 - requirements for local upgrade servers [21-29](#)
 - uploading
 - certificate files [11-7](#)
 - root certificates [11-3](#)
 - URL
 - Cisco IronPort Data Security Policies [15-6](#)
 - External DLP Policies [15-6](#)
 - Outbound Malware Scanning Policies [12-4](#)
 - URL categories [9-17](#)
 - abbreviations [9-22](#)
 - blocking [15-8](#)
 - descriptions [9-22](#)
 - uncategorized URLs [18-4](#)
 - URL Categories report [18-3](#)
 - URL category set
 - updates [9-4, 18-4, 21-3](#)
 - URL Filters
 - configuring [9-9](#)
 - custom categories [9-13](#)
 - database [9-3](#)
 - enabling [9-4](#)
 - no category [9-2](#)
 - regular expressions [9-20](#)
 - time based [9-19](#)
 - URL category descriptions [9-22](#)
 - viewing filtering activity [9-19](#)
 - URL submission tool
 - using [9-3](#)
 - user accounts
 - about [21-7](#)
 - managing [21-8](#)
 - user agents
 - Cisco IronPort Data Security Policies [15-7](#)
 - External DLP Policies [15-7](#)
 - Outbound Malware Scanning Policies [12-4](#)
 - user defined notification pages
 - example [16-3](#)
 - overview [16-8](#)
 - parameters [16-9](#)
 - user location
 - Cisco IronPort Data Security Policies [15-7](#)
 - External DLP Policies [15-7](#)
 - Outbound Malware Scanning Policies [12-4](#)
 - usernames
 - making unrecognizable in reports [17-1](#)
 - user passwords [21-9](#)
 - user preferences
 - defining [21-11](#)
-
- ## V
- validating
 - certificates [11-6](#)
 - variables
 - end-user notification pages [16-5](#)
 - VLAN
 - etherconfig command [3-25](#)
 - interfaceconfig command [3-27](#)
 - labels [3-25](#)
 - VMotion [2-1](#)
-
- ## W
- W3C access logs
 - overview [20-15](#)

warning page
 end-user URL category page [16-12](#)

warning users [9-17](#)
 configuring end-user warning page [16-12](#)
 using URL categories [9-17](#)

WBRS
 see also *Web Reputation Filters*

WCCP router
 WCCP services [3-21](#)

WCCP services
 adding [3-21](#)
 editing [3-21](#)
 IP spoofing [3-24](#)
 overview [3-21](#)

web browsers
 supported [1-3](#)

web interface
 browser requirements [1-3](#)
 navigating [1-3](#)

web proxy
 overview [5-16](#)

Web Reputation Filters
 about [13-2](#)
 access log file [13-13](#)
 configuring Access Policies [13-12](#)
 database [13-13](#)
 how it works [13-2](#)
 report [18-6](#)
 scores [13-2](#)

Webroot scanning engine
 database [13-13](#)
 overview [13-5](#)
 Threat Risk Threshold [13-8](#)

Web Sites report [18-3](#)

whitelist address
 see *known allowed address*

Y

YouTube
 headers [20-31](#)
YouTube, logging added headers for [20-31](#)

Z

zero day revocation
 defined [8-1](#)

