

# User Guide for AsyncOS 12.7 for Cisco Web Security Appliances - LD (Limited Deployment)

**First Published:** 2021-09-15

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



# CONTENTS


CHAPTER 1

**Introduction** 1

About Web Security Appliance 1

What's New in AsyncOS 12.7 1

Related Topics 1

Using the Appliance Web Interface 1

Web Interface Browser Requirements 2

Enabling Access to the Web Interface on Virtual Appliances 3

Accessing the Appliance Web Interface 3

Committing Changes in the Web Interface 4

Clearing Changes in the Web Interface 5

Supported Languages 5

The Cisco SensorBase Network 5

SensorBase Benefits and Privacy 6

Enabling Participation in The Cisco SensorBase Network 6

CHAPTER 2

**Connect, Install, and Configure** 7

Overview of Connect, Install, and Configure 7

Comparison of Modes of Operation 8

Task Overview - Connect, Install, and Configure 11

Connect the Appliance 11

Gathering Setup Information 14

System Setup Wizard 15

System Setup Wizard Reference Information 16

Network / System Settings 17

Network / Network Context 18

Network / Cloud Connector Settings 18

Network / Network Interfaces and Wiring 18
Network / Layer 4 Traffic Monitor Wiring 19
Network / Routes for Management and Data Traffic 19
Network / Transparent Connection Settings 20
Network /Administrative Settings 20
Security / Security Settings 21
Upstream Proxies 22
Upstream Proxies Task Overview 22
Creating Proxy Groups for Upstream Proxies 22
Network Interfaces 23
IP Address Versions 24
Enabling or Changing Network Interfaces 24
Network Interface Card Configuration 26
Media Settings on Ethernet Interfaces 26
Network Interface Card Pairing/Teaming 27
Enabling NIC Pairing using the etherconfig Command 28
Guidelines for Configuring NIC Pairing 35
Configuring Failover Groups for High Availability 36
Add Failover Group 37
Edit High Availability Global Settings 38
View Status of Failover Groups 38
Using the P2 Data Interface for Web Proxy Data 38
Configuring TCP/IP Traffic Routes 39
Outbound Services Traffic 40
Modifying the Default Route 41
Adding a Route 41
Saving and Loading Routing Tables 41
Deleting a Route 42
Configuring Transparent Redirection 42
Specifying a Transparent Redirection Device 42
Using An L4 Switch 43
Configuring WCCP Services 43
Increasing Interface Capacity Using VLANs 48
Configuring and Managing VLANs 48

Redirect Hostname and System Hostname 50
Changing the Redirect Hostname 50
Changing the System Hostname 51
Configuring SMTP Relay Host Settings 51
Configuring an SMTP Relay Host 51
DNS Settings 52
Split DNS 52
Clearing the DNS Cache 52
Editing DNS Settings 53
Troubleshooting Connect, Install, and Configure 54

CHAPTER 3 **Connect the Appliance to a Cisco Cloud Web Security Proxy 55**
How to Configure and Use Features in Cloud Connector Mode 55
Deployment in Cloud Connector Mode 55
Configuring the Cloud Connector 56
Controlling Web Access Using Directory Groups in the Cloud 59
Bypassing the Cloud Proxy Server 59
Partial Support for FTP and HTTPS in Cloud Connector Mode 60
Preventing Loss of Secure Data 60
Viewing Group and User Names and IP Addresses 60
Subscribing to Cloud Connector Logs 60
Identification Profiles and Authentication with Cloud Web Security Connector 61
Identifying Machines for Policy Application 62
Guest Access for Unauthenticated Users 62

CHAPTER 4 **Intercepting Web Requests 63**
Overview of Intercepting Web Requests 63
Tasks for Intercepting Web Requests 63
Best Practices for Intercepting Web Requests 64
Web Proxy Options for Intercepting Web Requests 65
Configuring Web Proxy Settings 65
Web Proxy Cache 68
Clearing the Web Proxy Cache 68
Removing URLs from the Web Proxy Cache 68

Specifying Domains or URLs that the Web Proxy never Caches 68
Choosing The Web Proxy Cache Mode 69
Web Proxy IP Spoofing 70
Creating IP Spoofing Profiles 71
Web Proxy Custom Headers 72
Adding Custom Headers To Web Requests 72
Web Proxy Bypassing 73
Web Proxy Bypassing for Web Requests 73
Configuring Web Proxy Bypassing for Web Requests 74
Configuring Web Proxy Bypassing for Applications 74
Web Proxy Usage Agreement 75
Domain Map 75
Domain Map for Specific Applications 75
Client Options for Redirecting Web Requests 77
Using PAC Files with Client Applications 77
Options For Publishing Proxy Auto-Config (PAC) Files 77
Client Options For Finding Proxy Auto-Config (PAC) Files 78
Automatic PAC File Detection 78
Hosting PAC Files on the Web Security Appliance 78
Specifying PAC Files in Client Applications 79
Configuring a PAC File Location Manually in Clients 79
Detecting the PAC File Automatically in Clients 80
FTP Proxy Services 80
Overview of FTP Proxy Services 80
Enabling and Configuring the FTP Proxy 81
SOCKS Proxy Services 82
Overview of SOCKS Proxy Services 82
Enabling Processing of SOCKS Traffic 83
Configuring the SOCKS Proxy 83
Creating SOCKS Policies 84
Troubleshooting Intercepting Requests 85

CHAPTER 5 **Acquire End-User Credentials** 87
Overview of Acquire End-User Credentials 87

Authentication Task Overview 87
Authentication Best Practices 88
Authentication Planning 89
Active Directory/Kerberos 89
Active Directory/Basic 90
Active Directory/NTLMSSP 91
LDAP/Basic 91
Identifying Users Transparently 92
Understanding Transparent User Identification 92
Rules and Guidelines for Transparent User Identification 95
Configuring Transparent User Identification 95
Using the CLI to Configure Advanced Transparent User Identification Settings 96
Configuring Single-Sign-on 96
Creating a Service Account in Windows Active Directory for Kerberos Authentication in High Availability Deployments 97
Authentication Realms 99
External Authentication 100
Configuring External Authentication through an LDAP Server 100
Enabling RADIUS External Authentication 100
Creating an Active Directory Realm for Kerberos Authentication Scheme 100
How to Create an Active Directory Authentication Realm (NTLMSSP and Basic) 104
Prerequisites for Creating an Active Directory Authentication Realm (NTLMSSP and Basic) 104
About Using Multiple NTLM Realms and Domains 105
Creating an Active Directory Authentication Realm (NTLMSSP and Basic) 105
Creating an LDAP Authentication Realm 107
Using Multiple NTLM Realms and Domains 112
About Deleting Authentication Realms 112
Configuring Global Authentication Settings 112
Authentication Sequences 117
About Authentication Sequences 117
Creating Authentication Sequences 118
Editing And Reordering Authentication Sequences 119
Deleting Authentication Sequences 119
Failed Authentication 119

About Failed Authentication 120
Bypassing Authentication with Problematic User Agents 120
Bypassing Authentication 121
Permitting Unauthenticated Traffic While Authentication Service is Unavailable 122
Granting Guest Access After Failed Authentication 122
Define an Identification Profile that Supports Guest Access 123
Use an Identification Profile that Supports Guest Access in a Policy 123
Configure How Guest User Details are Logged 123
Failed Authorization: Allowing Re-Authentication with Different Credentials 124
About Allowing Re-Authentication with Different Credentials 124
Allowing Re-Authentication with Different Credentials 124
Tracking Identified Users 125
Supported Authentication Surrogates for Explicit Requests 125
Supported Authentication Surrogates for Transparent Requests 125
Tracking Re-Authenticated Users 126
Credentials 126
Tracking Credentials for Reuse During a Session 126
Authentication and Authorization Failures 127
Credential Format 127
Credential Encryption for Basic Authentication 127
About Credential Encryption for Basic Authentication 127
Configuring Credential Encryption 128
Troubleshooting Authentication 128

CHAPTER 6 **Classify End-Users for Policy Application** 129
Overview of Classify Users and Client Software 129
Classify Users and Client Software: Best Practices 130
Identification Profile Criteria 130
Classifying Users and Client Software 131
Enable/Disable an Identity 136
Identification Profiles and Authentication 137
Troubleshooting Identification Profiles 138
Troubleshooting Surrogate Types in Identification Profiles 139

CHAPTER 7 SaaS Access Control 141

Overview of SaaS Access Control 141

Configuring the Appliance as an Identity Provider 142

Using SaaS Access Control and Multiple Appliances 144

Creating SaaS Application Authentication Policies 144

Configuring End-user Access to the Single Sign-on URL 146

CHAPTER 8 Integrate the Cisco Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) 149

Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service 149

About pxGrid 150

About the ISE/ISE-PIC Server Deployment and Failover 151

ISE/ISE-PIC Certificates 151

Using Self-signed Certificates 152

Using CA-signed Certificates 152

Fallback Authentication 152

Tasks for Integrating the ISE/ISE-PIC Service 153

Generating Certificate through ISE/ISE-PIC 154

Configuring ISE/ISE-PIC server for Web Security Appliance Access 154

Connect to the ISE/ISE-PIC Services 155

Import the Self-signed Web Security Appliance Client Certificate to ISE/ISE-PIC Standalone Deployment 157

Import the Self-signed Web Security Appliance Client Certificate to ISE/ISE-PIC Distributed Deployment 158

Configuring logging for ISE/ISE-PIC 159

Acquiring ISE/ISE-PIC ERS Server Details from ISE/ISE-PIC 160

Configure ISE-SXP Integration 160

About ISE-SXP Protocol for SGT-to-IP Address Mapping 161

Guidelines and Limitations 161

Prerequisites 161

Enabling ISE-SXP Protocol for SGT-to-IP Address Mapping 161

Verifying the ISE-SXP Protocol Configuration 162

VDI (Virtual Desktop Infrastructure) User Authentication in ISE/ISE-PIC Integrations 163

Troubleshooting Identity Services Engine Problems 163

CHAPTER 9 **Classify URLs for Policy Application** 165

Overview of Categorizing URL Transactions 165

Categorization of Failed URL Transactions 166

Enabling the Dynamic Content Analysis Engine 166

Uncategorized URLs 166

Matching URLs to URL Categories 167

Reporting Uncategorized and Misclassified URLs 167

URL Categories Database 168

Configuring the URL Filtering Engine 168

Managing Updates to the Set of URL Categories 168

Understanding the Impacts of URL Category Set Updates 169

Effects of URL Category Set Changes on Policy Group Membership 169

Effects of URL Category Set Updates on Filtering Actions in Policies 169

Merged Categories - Examples 172

Controlling Updates to the URL Category Set 172

Manually Updating the URL Category Set 173

Default Settings for New and Changed Categories 173

Verifying Existing Settings and/or Making Changes 174

Receiving Alerts About Category and Policy Changes 174

Responding to Alerts about URL Category Set Updates 174

Filtering Transactions Using URL Categories 175

Configuring URL Filters for Access Policy Groups 175

Exceptions to Blocking for Embedded and Referred Content 177

Configuring URL Filters for Decryption Policy Groups 178

Configuring URL Filters for Data Security Policy Groups 179

YouTube Categorization 181

Enabling the YouTube Categorization Feature 182

Creating and Editing Custom URL Categories 183

Address Formats and Feed-file Formats for Custom and External URL Categories 187

External Feed-file Formats 188

Filtering Adult Content 189

Enforcing Safe Searches and Site Content Ratings 190

Logging Adult Content Access 191

Redirecting Traffic in the Access Policies 191
Logging and Reporting 192
Warning Users and Allowing Them to Continue 192
Configuring Settings for the End-User Filtering Warning Page 193
Creating Time Based URL Filters 193
Viewing URL Filtering Activity 194
Understanding Unfiltered and Uncategorized Data 194
URL Category Logging in Access Logs 195
Regular Expressions 195
Forming Regular Expressions 195
Guidelines for Avoiding Validation Failures 196
Regular Expression Character Table 197
URL Category Descriptions 198

CHAPTER 10 **Create Policies to Control Internet Requests** 213
Overview of Policies: Control Intercepted Internet Requests 213
Intercepted HTTP/HTTPS Request Processing 214
Managing Web Requests Through Policies Task Overview 215
Managing Web Requests Through Policies Best Practices 215
Policies 215
Policy Types 215
Policy Order 218
Creating a Policy 219
Adding and Editing Secure Group Tags for a Policy 223
Adding Routing Destination and IP Spoofing Profile to Routing Policy 223
Policy Configuration 225
Access Policies: Blocking Objects 226
Archive Inspection Settings 229
Block, Allow, or Redirect Transaction Requests 230
Client Applications 231
About Client Applications 231
Using Client Applications in Policies 232
Defining Policy Membership Using Client Applications 232
Defining Policy Control Settings Using Client Applications 232

Exempting Client Applications from Authentication 233
Time Ranges and Quotas 233
Time Ranges for Policies and Acceptable Use Controls 233
Creating a Time Range 233
Time and Volume Quotas 234
Volume Quota Calculations 235
Time Quota Calculations 235
Defining Time and Volume Quotas 235
Access Control by URL Category 236
Using URL Categories to Identify Web Requests 236
Using URL Categories to Action Web Request 237
Remote Users 238
About Remote Users 238
How to Configure Identification of Remote Users 238
Configuring Identification of Remote Users 239
Display Remote User Status and Statistics for ASAs 240
Troubleshooting Policies 240

CHAPTER 11 **Create Decryption Policies to Control HTTPS Traffic 241**
Overview of Create Decryption Policies to Control HTTPS Traffic 241
Managing HTTPS Traffic through Decryption Policies Task Overview 242
Managing HTTPS Traffic through Decryption Policies Best Practices 242
Decryption Policies 242
Enabling the HTTPS Proxy 245
Controlling HTTPS Traffic 247
Configuring Decryption Options 248
Authentication and HTTPS Connections 249
Root Certificates 249
Managing Certificate Validation and Decryption for HTTPS 250
Valid Certificates 250
Invalid Certificate Handling 251
Uploading a Root Certificate and Key 251
Generating a Certificate and Key for the HTTPS Proxy 252
Configuring Invalid Certificate Handling 252

Options for Certificate Revocation Status Checking 253
Enabling Real-Time Revocation Status Checking 254
Trusted Root Certificates 255
Adding Certificates to the Trusted List 255
Removing Certificates from the Trusted List 255
Routing HTTPS Traffic 256
Troubleshooting Decryption/HTTPS/Certificates 256

CHAPTER 12 **Scan Outbound Traffic for Existing Infections** 257
Overview of Scanning Outbound Traffic 257
User Experience When Requests Are Blocked by the DVS Engine 257
Understanding Upload Requests 258
Criteria for Group Membership 258
Matching Client Requests to Outbound Malware Scanning Policy Groups 258
Creating Outbound Malware Scanning Policies 259
Controlling Upload Requests 261
Logging of DVS Scanning 262

CHAPTER 13 **Configuring Security Services** 263
Overview of Configuring Security Services 263
Overview of Web Reputation Filters 264
Web Reputation Scores 264
Understanding How Web Reputation Filtering Works 264
Web Reputation in Access Policies 265
Web Reputation in Decryption Policies 265
Web Reputation in Cisco Data Security Policies 266
Overview of Anti-Malware Scanning 266
Understanding How the DVS Engine Works 266
Working with Multiple Malware Verdicts 267
Webroot Scanning 267
McAfee Scanning 267
Matching Virus Signature Patterns 268
Heuristic Analysis 268
McAfee Categories 268

Sophos Scanning 268
Understanding Adaptive Scanning 269
Adaptive Scanning and Access Policies 269
Enabling Anti-Malware and Reputation Filters 269
Clearing the Advanced Malware Protection Services Cache 271
Configuring Anti-Malware and Reputation in Policies 271
Anti-Malware and Reputation Settings in Access Policies 272
Configuring Anti-Malware and Reputation Settings with Adaptive Scanning Enabled 272
Configuring Anti-Malware and Reputation Settings with Adaptive Scanning Disabled 273
Configuring Web Reputation Scores 274
Configuring Web Reputation Score Thresholds for Access Policies 274
Configuring Web Reputation Filter Settings for Decryption Policy Groups 275
Configuring Web Reputation Filter Settings for Data Security Policy Groups 275
Integrating the Appliance with AMP for Endpoints Console 276
Maintaining the Database Tables 278
The Web Reputation Database 278
Logging of Web Reputation Filtering Activity and DVS Scanning 278
Logging Adaptive Scanning 278
Caching 279
Malware Category Descriptions 279

CHAPTER 14 **File Reputation Filtering and File Analysis 281**
Overview of File Reputation Filtering and File Analysis 281
File Threat Verdict Updates 281
File Processing Overview 282
Supported Files for File Reputation and Analysis Services 283
Archive or Compressed File Processing 284
Privacy of Information Sent to the Cloud 285
Configuring File Reputation and Analysis Features 285
Requirements for Communication with File Reputation and Analysis Services 286
Routing Traffic to File Reputation and File Analysis Servers Through a Data Interface 286
Configuring an On-premises File Reputation Server 287
Configuring an On-Premises File Analysis Server 287
Enabling and Configuring File Reputation and Analysis Services 288

Important! Changes Needed in File Analysis Setting 292
(Public Cloud File Analysis Services Only) Configuring Appliance Groups 292
Which Appliances Are In the Analysis Group? 294
Configuring File Reputation and Analysis Service Action Per Access Policy 294
Ensuring That You Receive Alerts About Advanced Malware Protection Issues 294
Configuring Centralized Reporting for Advanced Malware Protection Features 295
File Reputation and File Analysis Reporting and Tracking 295
Identifying Files by SHA-256 Hash 296
File Reputation and File Analysis Report Pages 296
Viewing File Reputation Filtering Data in Other Reports 297
About Web Tracking and Advanced Malware Protection Features 297
Taking Action When File Threat Verdicts Change 298
Troubleshooting File Reputation and Analysis 299
Log Files 299
Several Alerts About Failure to Connect to File Reputation or File Analysis Servers 299
API Key Error (On-Premises File Analysis) 300
Files are Not Uploaded As Expected 300
File Analysis Details in the Cloud Are Incomplete 300
Alerts about File Types That Can Be Sent for Analysis 301

CHAPTER 15 **Managing Access to Web Applications** 303
Overview of Managing Access to Web Applications 303
Enabling the AVC Engine 304
AVC Engine Updates and Default Actions 304
User Experience When Requests Are Blocked by the AVC Engine 305
Policy Application Control Settings 305
Range Request Settings 306
Rules and Guidelines for Configuring Application Control 307
Configuring Application Control Settings in an Access Policy Group 308
Controlling Bandwidth 308
Configuring Overall Bandwidth Limits 309
Configuring User Bandwidth Limits 309
Configuring the Default Bandwidth Limit for an Application Type 310
Overriding the Default Bandwidth Limit for an Application Type 310

Configuring Bandwidth Controls for an Application 311
Controlling Instant Messaging Traffic 311
Viewing AVC Activity 311
AVC Information in Access Log File 312

CHAPTER 16 **Prevent Loss of Sensitive Data 313**
Overview of Prevent Loss of Sensitive Data 313
Bypassing Upload Requests Below a Minimum Size 314
User Experience When Requests Are Blocked As Sensitive Data 314
Managing Upload Requests 315
Managing Upload Requests on an External DLP System 316
Evaluating Data Security and External DLP Policy Group Membership 316
Matching Client Requests to Data Security and External DLP Policy Groups 316
Creating Data Security and External DLP Policies 317
Managing Settings for Upload Requests 319
URL Categories 320
Web Reputation 320
Content Blocking 320
Defining External DLP Systems 321
Configuring External DLP Servers 321
Controlling Upload Requests Using External DLP Policies 323
Logging of Data Loss Prevention Scanning 324

CHAPTER 17 **Notify End-Users of Proxy Actions 327**
End-User Notifications Overview 327
Configuring General Settings for Notification Pages 328
End-User Acknowledgment Page 328
Access HTTPS and FTP Sites with the End-User Acknowledgment Page 329
About the End-user Acknowledgment Page 329
Configuring the End-User Acknowledgment Page 330
End-User Notification Pages 332
Configuring On-Box End-User Notification Pages 332
Off-Box End-User Notification Pages 333
Displaying the Correct Off-Box Page Based on the Reason for Blocking Access 333

URL Criteria for Off-Box Notification Pages 333
Off-Box End-User Notification Page Parameters 334
Redirecting End-User Notification Pages to a Custom URL (Off-Box) 335
Configuring the End-User URL Filtering Warning Page 335
Configuring FTP Notification Messages 336
Custom Messages on Notification Pages 337
Supported HTML Tags in Custom Messages on Notification Pages 337
Caveats for URLs and Logos in Notification Pages 337
Editing Notification Page HTML Files Directly 338
Requirements for Editing Notification HTML Files Directly 338
Editing Notification HTML Files Directly 339
Using Variables in Notification HTML Files 340
Variables for Customizing Notification HTML Files 340
Notification Page Types 342

CHAPTER 18 **Generate Reports to Monitor End-user Activity** 353
Overview of Reporting 353
Working with Usernames in Reports 353
Report Pages 354
Using the Reporting Pages 355
Changing the Time Range 355
Choosing a Time Range for Reports 356
Searching Data 356
Choosing Which Data to Chart 357
Custom Reports 357
Modules That Cannot Be Added to Custom Reports 358
Creating Your Custom Report Page 358
Subdomains vs. Second-level Domains in Reporting and Tracking 358
Printing and Exporting Reports from Report Pages 359
Exporting Report Data 359
Using the Interactive Report Pages on the New Web Interface 360
Enabling Reporting 360
Scheduling Reports 361
Adding a Scheduled Report 362

Editing Scheduled Reports 362
Deleting Scheduled Reports 362
Generating Reports On Demand 363
Archived Reports 363
Troubleshooting L4 Traffic Monitor Reports 364

CHAPTER 19 **Secure Appliance Reports** 365
Overview Page 365
Users Page 367
User Details Page 367
User Count Page 368
Web Sites Page 368
URL Categories Page 369
URL Category Set Updates and Reports 369
Application Visibility Page 370
Anti-Malware Page 370
Malware Category Report Page 370
Malware Threat Report Page 371
Advanced Malware Protection Page 371
File Analysis Page 371
AMP Verdict Updates Page 371
Client Malware Risk Page 371
Client Detail Page for Web Proxy - Clients by Malware Risk 372
Web Reputation Filters Page 372
L4 Traffic Monitor Page 372
SOCKS Proxy Page 373
Reports by User Location Page 373
Web Tracking Page 374
Searching for Transactions Processed by the Web Proxy 374
Searching for Transactions Processed by the L4 Traffic Monitor 377
Searching for Transactions Processed by the SOCKS Proxy 377
System Capacity Page 378
System Status Page 378

CHAPTER 20 **Secure Appliance Reports on the New Web Interface** 381

Understanding the Web Reporting Pages on the New Web Interface 381

About Time Spent 383

Overview Page 384

Application Visibility Page 385

Layer 4 Traffic Monitor Page 387

SOCKS Proxy Page 389

URL Categories Page 390

Reducing Uncategorized URLs 391

URL Category Set Updates and Reports 391

Using The URL Categories Page in Conjunction with Other Reporting Pages 391

Reporting Misclassified and Uncategorized URLs 392

HTTPS Reports Page 392

Users Page 393

User Details Page (Web Reporting) 394

Web Sites Page 396

Advanced Malware Protection Page 397

Advanced Malware Protection - AMP Summary Page 398

Advanced Malware Protection - File Analysis Page 398

Anti-Malware Page 399

Malware Category Report Page 400

Malware Threat Report 400

Malware Category Descriptions 400

Client Malware Risks Page 402

Web Reputation Filters Page 402

(Web Reports Only) Choosing Which Data to Chart 404

Web Tracking on the New Web Interface 405

Searching for Transactions Processed by Web Proxy Services 405

Malware Category Descriptions 408

Searching for Transactions Processed by the Layer 4 Traffic Monitor 409

Searching for Transactions Processed by the SOCKS Proxy 409

Working with Web Tracking Search Results 410

Displaying More Web Tracking Search Results 410

Understanding Web Tracking Search Results 410
Viewing Transaction Details for Web Tracking Search Results 411
About Web Tracking and Upgrades 411
Scheduling and Archiving Web Reports on the New Web Interface 411
Scheduling Web Reports on the New Web Interface 411
Adding Scheduled Web Reports on the New Web Interface 412
Editing Scheduled Web Reports on the New Web Interface 413
Deleting Scheduled Web Reports on the New Web Interface 413
Archiving Web Reports on the New Web Interface 413
[New Web Interface] Generating Web Reports on Demand 413
System Status Page on the New Web Interface 414
Status 414
Services 416

CHAPTER 21 **Detecting Rogue Traffic on Non-Standard Ports** 419
Overview of Detecting Rogue Traffic 419
Configuring the L4 Traffic Monitor 419
List of Known Sites 420
Configuring L4 Traffic Monitor Global Settings 420
Updating L4 Traffic Monitor Anti-Malware Rules 421
Creating a Policy to Detect Rogue Traffic 421
Valid Formats 422
Viewing L4 Traffic Monitor Activity 422
Monitoring Activity and Viewing Summary Statistics 422
L4 Traffic Monitor Log File Entries 423

CHAPTER 22 **Monitor System Activity Through Logs** 425
Overview of Logging 425
Common Tasks for Logging 426
Best Practices for Logging 426
Troubleshooting Web Proxy Issues Using Logs 426
Log File Types 427
Adding and Editing Log Subscriptions 432
Deanonymizing W3C Log Fields 437

Pushing Log Files to Another Server 437
Archiving Log Files 438
Log File Names and Appliance Directory Structure 439
Reading and Interpreting Log Files 439
Viewing Log Files 440
Web Proxy Information in Access Log Files 440
Transaction Result Codes 444
ACL Decision Tags 445
Interpreting Access Log Scanning Verdict Entries 451
W3C Compliant Access Log Files 458
W3C Field Types 458
Interpreting W3C Access Logs 458
W3C Log File Headers 458
W3C Field Prefixes 459
Customizing Access Logs 460
Access Log User Defined Fields 460
Customizing Regular Access Logs 460
Customizing W3C Access Logs 461
Configuring Cisco CTA-specific Custom W3C Logs 462
Configuring Cisco Cloudlock-specific Custom W3C Logs 463
Traffic Monitor Log Files 464
Interpreting Traffic Monitor Logs 464
Log File Fields and Tags 465
Access Log Format Specifiers and W3C Log File Fields 465
Malware Scanning Verdict Values 477
Troubleshooting Logging 478

CHAPTER 23 **Integrating with Cisco Threat Response** 479
Integrating the Appliance with Cisco Threat Response 479
Performing Threat Analysis using Casebooks 481
Obtaining Client ID and Client Password Credentials 482
Adding Observable to Casebook for Threat Analysis 483
Improving User Experience of Cisco Web Security Appliance using Cisco Success Network 484
Enabling and Registering Cisco Success Network on the appliance 487

Disabling Cisco Success Network 488

CHAPTER 24 **Perform System Administration Tasks 489**

Overview of System Administration 489

Saving, Loading, and Resetting the Appliance Configuration 490

Viewing and Printing the Appliance Configuration 490

Saving the Appliance Configuration File 490

Loading the Appliance Configuration File 491

Resetting the Appliance Configuration to Factory Defaults 492

Saving Configuration File Backup 492

Cisco Web Security Appliance Licensing 493

Working with Feature Keys 493

Displaying and Updating Feature Keys 493

Changing Feature Key Update Settings 494

Smart Software Licensing 494

Overview 494

Enabling Smart Software Licensing 496

Registering the Appliance with Cisco Smart Software Manager 497

Requesting for Licenses 499

Deregistering the Appliance from Smart Cisco Software Manager 500

Reregistering the Appliance with Smart Cisco Software Manager 501

Changing Transport Settings 501

Renewing Authorization and Certificate 501

Updating Smart Agent 502

Alerts 502

Command Line Interface 503

Virtual Appliance License 507

Installing a Virtual Appliance License 508

Enabling Remote Power Cycling 508

Administering User Accounts 509

Managing Local User Accounts 509

Adding Local User Accounts 510

Deleting User Accounts 511

Editing User Accounts 511

Changing Passphrases 511
Configuring Restrictive User Account and Passphrase Settings 511
RADIUS User Authentication 512
Sequence of Events For Radius Authentication 512
Enabling External Authentication Using RADIUS 512
Defining User Preferences 513
Configuring Administrator Settings 514
Setting Passphrase Requirements for Administrative Users 514
Additional Security Settings for Accessing the Appliance 515
User Network Access 516
Resetting the Administrator Passphrase 517
Configuring the Return Address for Generated Messages 518
Managing Alerts 518
Alert Classifications and Severities 518
Alert Classifications 518
Alert Severities 519
Managing Alert Recipients 519
Adding and Editing Alert Recipients 519
Deleting Alert Recipients 519
Configuring Alert Settings 519
Alert Listing 520
Hardware Alerts 520
System Alerts 521
Updater Alerts 526
Anti-Malware Alerts 526
AMP Alerts 526
Web Proxy Alerts 527
External URL Categories Alerts 528
L4 Traffic Monitor Alerts 528
Policy Expiration Alerts 528
FIPS Compliance 529
FIPS Certificate Requirements 529
FIPS Certificate Validation 530
Enabling or Disabling FIPS Mode 530

System Date and Time Management 531
Setting the Time Zone 531
Synchronizing the System Clock with an NTP Server 531
SSL Configuration 532
Certificate Management 533
Strict Certificate Validation 534
About Certificates and Keys 534
Managing Trusted Root Certificates 535
Certificate Updates 535
Viewing Blocked Certificates 536
Uploading or Generating a Certificate and Key 536
Uploading a Certificate and Key 536
Generating a Certificate and Key 537
Certificate Signing Requests 537
Intermediate Certificates 538
AsyncOS for Web Upgrades and Updates 538
Best Practices For Upgrading AsyncOS for Web 538
Upgrading and Updating AsyncOS and Security Service Components 539
Downloading and Installing an Upgrade 539
Viewing Status of, Canceling, or Deleting a Background Download 540
Automatic and Manual Update and Upgrade Queries 541
Manually Updating Security Service Components 541
Local And Remote Update Servers 542
Updating and Upgrading from the Cisco Update Servers 542
Upgrading from a Local Server 543
Differences Between Local and Remote Upgrading Methods 544
Configuring Upgrade and Service Update Settings 545
Reverting to a Previous Version of AsyncOS for Web 546
Reverting AsyncOS on Virtual Appliances Impacts the License 546
Configuration File Use in the Revert Process 546
Reverting AsyncOS for an Appliance Managed by the SMA 546
Reverting AsyncOS for Web to a Previous Version 547
Monitoring System Health and Status Using SNMP 548
MIB Files 548

Enabling and Configuring SNMP Monitoring 549
Hardware Objects 549
SNMP Traps 549
About the connectivityFailure SNMP Trap 550
CLI Example: snmpconfig 550
Web Traffic Tap 552
Enabling Web Traffic Tap 553
Configuring Web Traffic Tap Policies 554

APPENDIX A **Troubleshooting** 555
General Troubleshooting Best Practices 555
FIPS Mode Problems 556
CSP Encryption 556
Certificate Validation 556
Authentication Problems 556
Troubleshooting Tools for Authentication Issues 557
Failed Authentication Impacts Normal Operations 557
LDAP Problems 557
LDAP User Fails Authentication due to NTLMSSP 557
LDAP Authentication Fails due to LDAP Referral 557
Basic Authentication Problems 558
Basic Authentication Fails 558
Single Sign-On Problems 558
Users Erroneously Prompted for Credentials 558
Blocked Object Problems 558
Some Microsoft Office Files Not Blocked 558
Blocking DOS Executable Object Types Blocks Updates for Windows OneCare 559
Browser Problems 559
WPAD Not Working With Firefox 559
DNS Problems 559
Alert: Failed to Bootstrap the DNS Cache 559
Failover Problems 559
Failover Misconfiguration 560
Failover Issues on Virtual Appliances 560

Feature Keys Expired 560
FTP Problems 560
URL Categories Do Not Block Some FTP Sites 560
Large FTP Transfers Disconnect 561
Zero Byte File Appears On FTP Servers After File Upload 561
Chrome Browser Not Detected As User Agent in FTP-over-HTTP Requests 561
Upload/Download Speed Issues 561
Hardware Issues 562
Cycling Appliance Power 562
Appliance Health and Status Indicators 562
Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware 563
HTTPS/Decryption/Certificate Problems 563
Accessing HTTPS Sites Using Routing Policies with URL Category Criteria 563
HTTPS Request Failures 563
HTTPS with IP-based Surrogates and Transparent Requests 563
Different Client “Hello” Behavior for Custom and Default Categories 564
Bypassing Decryption for Particular Websites 564
Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content 564
Alert: Problem with Security Certificate 565
Identity Services Engine Problems 565
Tools for Troubleshooting ISE Issues 565
ISE Server Connection Issues 566
Certificate Issues 566
Network Issues 567
Other ISE Server Connectivity Issues 567
ISE-related Critical Log Messages 568
Problems with Custom and External URL Categories 568
Issues Downloading An External Live Feed File 569
MIME Type Issue on IIS Server for .CSV Files 569
Malformed Feed File Following Copy and Paste 570
Logging Problems 570
Custom URL Categories Not Appearing in Access Log Entries 570
Logging HTTPS Transactions 570
Alert: Unable to Maintain the Rate of Data Being Generated 570

Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs 571
Policy Problems 571
Access Policy not Configurable for HTTPS 571
Blocked Object Problems 571
Some Microsoft Office Files Not Blocked 572
Blocking DOS Executable Object Types Blocks Updates for Windows OneCare 572
Identification Profile Disappeared from Policy 572
Policy Match Failures 572
Policy is Never Applied 572
HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication 572
User Matches Global Policy for HTTPS and FTP over HTTP Requests 573
User Assigned Incorrect Access Policy 573
Policy Trace Mismatch after Modifying Policy Parameters 573
Policy Troubleshooting Tool: Policy Trace 573
About the Policy Trace Tool 574
Tracing Client Requests 574
Advanced: Request Details 575
Advanced: Response Detail Overrides 576
Problems with File Reputation and File Analysis 577
Reboot Issues 577
Virtual Appliance Running on KVM Hangs on Reboot 577
Hardware Appliances: Remotely Resetting Appliance Power 577
Site Access Problems 578
Cannot Access URLs that Do Not Support Authentication 578
Cannot Access Sites With POST Requests 579
Upstream Proxy Problems 579
Upstream Proxy Does Not Receive Basic Credentials 579
Client Requests Fail Upstream Proxy 579
Unable to Route FTP Requests Via an Upstream Proxy 580
Virtual Appliances 580
Do Not Use Force Reset, Power Off, or Reset Options During AsyncOS Startup 580
Network Connectivity on KVM Deployments Works Initially, Then Fails 580
Slow Performance, Watchdog Issues, and High CPU Usage on KVM Deployments 580

General Troubleshooting for Virtual Appliances Running on Linux Hosts 580
WCCP Problems 581
Maximum Port Entries 581
Packet Capture 581
Starting a Packet Capture 581
Managing Packet Capture Files 582
Downloading or Deleting Packet Capture Files 582
Working With Support 583
Gathering Information for Efficient Service 583
Opening a Technical Support Request 583
Getting Support for Virtual Appliances 584
Enabling Remote Access to the Appliance 584

APPENDIX B **Command Line Interface** 587
Overview of the Command Line Interface 587
Accessing the Command Line Interface 587
First Access 587
Subsequent Access 588
Working with the Command Prompt 588
Command Syntax 588
Select Lists 589
Yes/No Queries 589
Subcommands 589
Escaping Subcommands 589
Command History 589
Completing Commands 590
Committing Configuration Changes Using the CLI 590
General Purpose CLI Commands 590
CLI Example: Committing Configuration Changes 590
CLI Example: Clearing Configuration Changes 590
CLI Example: Exiting the Command Line Interface Session 591
CLI Example: Seeking Help on the Command Line Interface 591
Web Security Appliance CLI Commands 591

APPENDIX C **Additional Information** 613

Cisco Notification Service 613

Documentation Set 613

Training 614

Knowledge Base Articles (TechNotes) 614

Cisco Support Community 614

Customer Support 614

Registering for a Cisco Account to Access Resources 615

Cisco Welcomes Your Comments 615

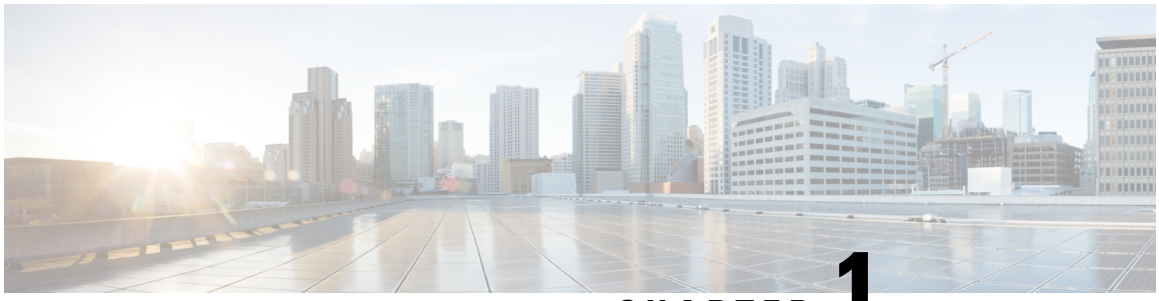
Third Party Contributors 615

Handling Personally Identifiable Information 615

APPENDIX D **End User License Agreement** 617

Cisco Systems End User License Agreement 617

Supplemental End User License Agreement for Cisco Systems Content Security Software 623



CHAPTER 1

# Introduction

This topic contains the following sections:


- About Web Security Appliance , on page 1
- What's New in AsyncOS 12.7, on page 1
- Related Topics, on page 1
- Using the Appliance Web Interface, on page 1
- Supported Languages, on page 5
- The Cisco SensorBase Network, on page 5


## About Web Security Appliance

## What's New in AsyncOS 12.7

*Table 1: What's New in AsyncOS 12.7*

| Feature | Description |
|---|---|
| ISE-SXP integration | You can integrate ISE-SXP deployment with Cisco Web Security Appliance for passive authentication. This allows you to get all defined mappings, including SGT-to-IP address mappings that are published through SXP.<br>See Configure ISE-SXP Integration, on page 160. |

## Related Topics

- http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html

## Using the Appliance Web Interface


- Web Interface Browser Requirements, on page 2

- Enabling Access to the Web Interface on Virtual Appliances , on page 3
- Accessing the Appliance Web Interface, on page 3
- Committing Changes in the Web Interface, on page 4
- Clearing Changes in the Web Interface, on page 5


# Web Interface Browser Requirements

Following are the requirements for accessing the web interface:

- Cookies and JavaScript must be supported and enabled by your browser.
- The browser must be able to render HTML pages that contain 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** Use only 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.

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

***Table 2: Supported Browsers and Releases***

| Browser | Windows 10 | MacOS 10.6 |
|---|---|---|
| Safari | — | 7.0 and later |
| Google Chrome | Latest stable version | Latest stable version |
| Microsoft Internet Explorer | 11.0 | — |
| Mozilla Firefox | Latest stable version | Latest stable version |
| Microsoft Edge | Latest stable version | Latest stable version |

Browsers are supported only for operating systems officially supported by the browser.

You may need to configure your browser's pop-up blocking settings in order to use the GUI, because some buttons or links in the interface will cause additional windows to open.

You can access the legacy web interface of the appliance on any of the supported browsers.

The supported resolution for the new web interface of the appliance (AsyncOS 11.8 and later) is between 1280x800 and 1680x1050. The best viewed resolution for all supported browsers is 1440x900.

**Note** Cisco does not recommend viewing the new web interface of the appliance on higher resolutions.

# Enabling Access to the Web Interface on Virtual Appliances

By default, the HTTP and HTTPS interfaces are not enabled on virtual appliances. To enable these protocols, you must use the command-line interface.

### Procedure

**Step 1** Access the command-line interface. See Accessing the Command Line Interface, on page 587.

**Step 2** Run the `interfaceconfig` command.

Press Enter at a prompt to accept the default value.

Look for the prompts for HTTP and HTTPS and enable the protocol(s) that you will use.

Look for the prompts for AsyncOS API (Monitoring) for HTTP and HTTPS and enable the protocol(s) that you will use.

# Accessing the Appliance Web Interface

If you are using a virtual appliance, see Enabling Access to the Web Interface on Virtual Appliances , on page 3.

### Procedure

**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 host name) 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** [New Web Interface Only] Login to the legacy web interface and click **Web Security Appliance is getting a new look. Try it!!** link to access the new web interface. When you click this link, it opens a new tab in your web browser and goes to `https://wsa_appliance.com:<trailblazer-https-port>/ng-login`, where `wsa_appliance.com` is the appliance host name and `<trailblazer-https-port>` is the trailblazer HTTPS port configured on the appliance.

**Note**

- You must login to the legacy web interface of the appliance.
- By default, the new web interface needs TCP ports 6080, 6443 and 4431 to be operational. Ensure that these ports are not blocked in the enterprise firewall.
- The default port for accessing new web interface is 4431. This can be customized using `trailerblazerconfig` CLI command. For more information on the `trailblazerconfig` CLI command, see Web Security Appliance CLI Commands, on page 591.
- The new web interface also needs AsyncOS API (Monitoring) ports for HTTP and HTTPS. By default these ports are 6080 and 6443. The AsyncOS API (Monitoring) ports can also be customized in the `interfaceconfig` CLI command. For more information on the `interfaceconfig` CLI command, see Web Security Appliance CLI Commands, on page 591.

  **Note**
  The ports are enabled by default, but once these ports are disabled, they will be enabled again after the upgrade.

- If you change these default ports, then ensure that the customized ports for the new web interface too must not be blocked in the enterprise firewall.

**Step 3** When the appliance login screen appears, enter your user name and passphrase to access the appliance.

By default, the appliance ships with the following user name and passphrase:

- User name: **admin**
- Passphrase: **ironport**

If this is the first time you have logged in with the default **admin** user name, you will be prompted to immediately change the passphrase.

**Step 4** To view a listing of recent appliance access attempts, both successes and failures, for your user name, click the recent-activity icon (**i** or **!** for success or failure respectively) in front of the "Logged in as" entry in the upper right corner of the application window.

# Committing Changes in the Web Interface

**Procedure**

**Step 1** Click **Commit Changes**.

**Step 2** Enter comments in the Comment field if you choose.

**Step 3** Click **Commit Changes**.

**Note**

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

## Clearing Changes in the Web Interface

**Procedure**

**Step 1** Click **Commit Changes**.

**Step 2** Click **Abandon Changes**.

# Supported Languages

AsyncOS can display its GUI and CLI in any of the following languages:

- German
- English
- Spanish
- French
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Chinese
- Taiwanese

# 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 Cisco 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 passphrases. 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.

**Procedure**

**Step 1** Choose **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:

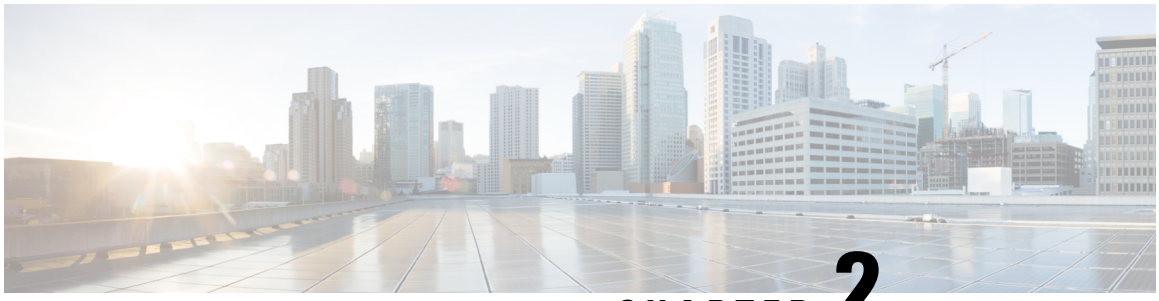
- **Limited.** Basic participation summarizes server name information and sends MD5-hashed path segments to the SensorBase Network servers.
- **Standard.** Enhanced participation sends the entire URL with unobfuscated path segments to the SensorBase Network servers. This option assists in providing a 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 Cisco 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.



CHAPTER 2

# Connect, Install, and Configure

This topic contains the following sections:


- Overview of Connect, Install, and Configure, on page 7
- Deploying a Virtual Appliance , on page 8
- Comparison of Modes of Operation, on page 8
- Task Overview - Connect, Install, and Configure, on page 11
- Connect the Appliance, on page 11
- Gathering Setup Information, on page 14
- System Setup Wizard, on page 15
- Upstream Proxies, on page 22
- Network Interfaces, on page 23
- Configuring Failover Groups for High Availability, on page 36
- Using the P2 Data Interface for Web Proxy Data , on page 38
- Redirect Hostname and System Hostname, on page 50
- DNS Settings, on page 52
- Troubleshooting Connect, Install, and Configure, on page 54


# Overview of Connect, Install, and Configure

The Web Security Appliance  provides the following modes of operation:

- Standard: The Standard mode of Web Security Appliance  operation includes on-site Web Proxy services and Layer-4 traffic monitoring, which are not available in the Cloud Web Security Connector mode.
- Cloud Web Security Connector: In Cloud Web Security Connector mode, the appliance connects to and routes traffic to a Cisco Cloud Web Security (CWS) proxy, where Web security policies are enforced.

The appliance has 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 lets you set up basic services and settings, while the appliance's Web interface lets you modify settings and configure additional options.

# Deploying a Virtual Appliance

To deploy a virtual Web Security Appliance , see the *Cisco Content Security Virtual Appliance Installation Guide* , available from
http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html

## Migrating from a Physical to a Virtual Appliance

To migrate your deployment from a physical appliance to a virtual appliance, see the virtual appliance installation guide referenced in the previous topic and the Release Notes for your AsyncOS version.

# Comparison of Modes of Operation

The following table presents the various menu commands available in Standard and Cloud connector Modes, thereby indicating the various features available in each mode.

| Menu | Available in Standard Mode | Available in Cloud Connector Mode |
|---|---|---|
| Reporting | System Status<br>Overview<br>Users<br>User Count<br>Web Sites<br>URL Categories<br>Application Visibility<br>Anti-Malware<br>Advanced Malware Protection<br>File Analysis<br>AMP Verdict Updates<br>Client Malware Risk<br>Web Reputation Filters<br>Layer-4 Traffic Monitor<br>Reports by User Location<br>Web Tracking<br>System Capacity<br>System Status<br>Scheduled Reports<br>Archived Reports | System Status |

| Menu | Available in Standard Mode | Available in Cloud Connector Mode |
|---|---|---|
| Web Security Manager | Identification Profiles<br>Cloud Routing Policies<br>SaaS Policies<br>Decryption Policies<br>Routing Policies<br>Access Policies<br>Overall Bandwidth Limits<br>Cisco Data Security<br>Outbound Malware Scanning<br>External Data Loss Prevention<br>Web Traffic Tap Policies<br>SOCKS Policies<br>Custom URL Categories<br>Define Time Ranges and Quotas<br>Bypass Settings<br>Layer-4 Traffic Monitor | Identification Profiles<br>Cloud Routing Policies<br>External Data Loss Prevention<br>Custom URL Categories |
| Security Services | Web Proxy<br>FTP Proxy<br>HTTPS Proxy<br>SOCKS Proxy<br>PAC File Hosting<br>Acceptable Use Controls<br>Anti-Malware and Reputation<br>Data Transfer Filters<br>AnyConnect Secure Mobility<br>End-User Notification<br>L4 Traffic Monitor<br>SensorBase<br>Reporting<br>Cisco Cloudlock<br>Cisco Cognitive Threat Analytics | Web Proxy |

| Menu | Available in Standard Mode | Available in Cloud Connector Mode |
|---|---|---|
| Network | Interfaces<br>Transparent Redirection<br>Routes<br>DNS<br>High Availability<br>Internal SMTP Relay<br>Upstream Proxy<br>External DLP Servers<br>Web Traffic Tap<br>Certificate Management<br>Authentication<br>Identity Provider for SaaS<br>Identity Services Engine | Interfaces<br>Transparent Redirection<br>Routes<br>DNS<br>High Availability<br>Internal SMTP Relay<br>External DLP Servers<br>Certificate Management<br>Authentication<br>Machine ID Service<br>Cloud Connector |
| System Administration | Policy Trace<br>Alerts<br>Log Subscriptions<br>Return Addresses<br>SSL Configuration<br>Users<br>Network Access<br>Time Zone<br>Time Settings<br>Configuration Summary<br>Configuration File<br>Feature Keys Settings<br>Feature Keys<br>Upgrade and Update Settings<br>System Upgrade<br>System Setup Wizard<br>FIPS Mode<br>Next Steps | Alerts<br>Log Subscriptions<br>SSL Configuration<br>Users<br>Network Access<br>Time Zone<br>Time Settings<br>Configuration Summary<br>Configuration File<br>Feature Keys<br>Upgrade and Update Settings<br>System Upgrade<br>System Setup Wizard |

| Menu | Available in Standard Mode | Available in Cloud Connector Mode |
|---|---|---|
| Cisco CWS Portal(available only in Hybrid Web Security mode) | N/A | N/A |

# Task Overview - Connect, Install, and Configure

| Task | More Information |
|---|---|
| Connect the appliance to Internet traffic. | Connect the Appliance, on page 11 |
| Gather and record set-up information. | Gathering Setup Information, on page 14 |
| Run the System Setup Wizard. | System Setup Wizard, on page 15 |
| Configure HTTPS proxy settings, Authentication Realms and Identification Profiles. This step must be completed for Hybrid Web Security mode. | Enabling the HTTPS Proxy, on page 245<br>Authentication Realms, on page 99<br>Identification Profiles and Authentication , on page 137 |
| (Optional) Connect upstream proxies. | Upstream Proxies, on page 22 |

# Connect the Appliance

### Before you begin

- To mount the appliance, cable the appliance for management, and connect the appliance to power, follow the instructions in the hardware guide for your appliance. For the location of this document for your model, see Documentation Set, on page 613.
- 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.

### Procedure

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

| Ethernet Port | Notes |
|---|---|
| M1 | Connect M1 to where it can:<br>• Send and receive Management traffic.<br>• (Optional) Send and receive web proxy data traffic.<br>You can connect a laptop directly to M1 to administer the appliance.<br>To connect to the management interface using a hostname (http://hostname:8080), add the appliance hostname and IP address to your DNS server database. |
| P1 and P2 (optional) | • Available for outbound management services traffic but not administration.<br>• Enable **Use M1 port for management only** (Network > Interfaces page).<br>• 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 | P1 only:<br>• Enable **Use M1 port for management only**.<br>• Connect P1 and M1 to different subnets.<br>• Use a duplex cable to connect P1 the internal network and the internet to receive both inbound and outbound traffic.<br>P1 and P2<br>• Enable P1.<br>• Connect M1, P1, and P2 to different subnets.<br>• Connect P2 to the internet to receive inbound internet traffic.<br>After running the System Setup Wizard, enable P2. | Device: WCCP v2 router:<br>• For Layer 2 redirection, physically connect router to P1/P2.<br>• For Layer 3 redirection, be aware of possible performance issues with Generic Routing Encapsulation.<br>• Create a WCCP Service on the appliance.<br>Device: Layer-4 Switch:<br>• For Layer 2 redirection, physically connect switch to P1/P2.<br>• For Layer 3 redirection, be aware of possible performance issues with Generic Routing Encapsulation.<br>**Note**<br>The appliance does not support inline mode. |
| M1 (optional) | If **Use M1 port for management 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 | To allow Layer-4 Traffic Monitor blocking, put Layer 4 Traffic Monitor on the same network as the Web Security Appliance .<br>**Recommended configuration:**<br>**Device: Network TAP:**<br>• **Connect T1 to network TAP to receive outbound client traffic.**<br>• **Connect T2 to network TAP to receive inbound internet traffic.**<br>Other options:<br>Device: Network TAP:<br>• Use duplex cable on T1 to receive inbound and outbound traffic.<br>Device: Spanned or mirrored port on a switch<br>• Connect T1 to receive outbound client traffic and connect T2 to receive inbound internet traffic.<br>• (Less preferred) Connect T1 using a half or full duplex cable to receive both inbound and outbound traffic.<br>Device: Hub:<br>• (Least preferred) Connect T1 using a duplex cable to receive both inbound and outbound traffic.<br>The appliance listens to traffic on all TCP ports on these interfaces. |

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

### What to do next

Gathering Setup Information, on page 14

### Related Topics


- Enabling or Changing Network Interfaces, on page 24
- Using the P2 Data Interface for Web Proxy Data , on page 38
- Adding and Editing a WCCP Service, on page 45
- Configuring Transparent Redirection, on page 42
- Upstream Proxies, on page 22

# 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, on page 16.

| **System Setup Wizard Worksheet** | | | |
|---|---|---|---|
| **Property** | **Value** | **Property** | **Value** |
| **Appliance Details** | | **Routes** | |
| Default SystemHostname | | **Management Traffic** | |
| **Local DNS Server(s)**<br>**(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 Passphrase | |
| **Management (M1) Port** | | **Administrative Settings** | |
| IPv4 Address (required)<br>IPv6 Address (optional) | | Administrator Passphrase | |
| Network Mask | | Email System Alerts To | |

| System Setup Wizard Worksheet | | | |
|---|---|---|---|
| **Property** | **Value** | **Property** | **Value** |
| Hostname | | (Optional) SMTP Relay Host | |
| **(Optional) Data (P1) Port** | | | |
| IPv4 (optional)<br>IPv6 Address (optional) | | | |
| Network Mask | | | |
| Hostname | | | |

# System Setup Wizard

### Before you begin

- Connect the Appliance to networks and devices. See Connect the Appliance, on page 11.
- Complete the System Setup Wizard worksheet. See Gathering Setup Information, on page 14.
- If you are setting up a virtual appliance:
  - Use the `loadlicense` command to load the virtual appliance license. For complete information, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.
  - Enable the HTTP and/or HTTPS interfaces: In the command-line interface (CLI), run the `interfaceconfig` command.
- While setting up System Setup Wizard, if Smart License is enabled, cloud service settings will also be enabled, redirecting you to the Cloud Services Settings page.
- Note that reference information for each configuration item used in the System Setup Wizard is available at System Setup Wizard Reference Information, on page 16.

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

### Procedure

**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 user name and passphrase to access the appliance. By default, the appliance ships with the following user name and passphrase:

- User name: `admin`
- Passphrase: `ironport`

**Step 3** You must immediately change the passphrase.

**Step 4** Choose **System Administration > System Setup Wizard**.

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, check **Reset Network Settings**, and then click the **Reset Configuration** button. The appliance will reset and the browser will refresh to the appliance home screen.

**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 reference tables provided in the following sections as required. See System Setup Wizard Reference Information, on page 16.

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

**Step 9** Click **Install This Configuration**.

### What to do next

A *Next Steps* page should appear once the configuration installed. However, depending on the IP, host name, or DNS settings you configured during setup, you may lose connection to the appliance at this stage. If a "page not found" error 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, on page 17
- Network / Network Interfaces and Wiring, on page 18
- Network / Routes for Management and Data Traffic, on page 19
- Network / Transparent Connection Settings, on page 20
- Network /Administrative Settings , on page 20

# Network / System Settings

| Property | Description |
|---|---|
| Default System Hostname | The system hostname is the fully-qualified hostname used to identify the appliance in the following areas:<br>• the command line interface (CLI)<br>• system alerts<br>• end-user notification and acknowledgment pages<br>• when forming the machine NetBIOS name when the Web Security Appliance joins an Active Directory domain<br>The system hostname does not correspond directly to interface hostnames and is not used by clients to connect to the appliance. |
| DNS Server(s) | • **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.<br>**Note**<br>Internet Root DNS servers will not resolve local host names. If you need the appliance to resolve local host names you must use a local DNS server, or add the appropriate static entries to the local DNS using the CLI.<br>• **Use these DNS Servers** – Provide address(es) for the local DNS server(s) that the appliance can use to resolve host names.<br>See DNS Settings, on page 52 for more information about these settings. |
| NTP Server | The Network Time Protocol (NTP) server used to synchronize the system clock with other servers on the network or the Internet.<br>The default is time.sco.cisco.com. |
| Time Zone | Provide time-zone information for location of the appliance; affects timestamps in message headers and log files. |
| Appliance Mode of Operation | • **Standard** – Used for standard on-premise policy enforcement.<br>• **Cloud Web Security Connector** – Used primarily to direct traffic to Cisco's Cloud Web Security service for policy enforcement and threat defense.<br>• **Hybrid Web Security** – Used in conjunction with Cisco's Cloud Web Security service for cloud and on-premise policy enforcement and threat defense.<br>See Comparison of Modes of Operation, on page 8 for more information about these modes of operation. |

## 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.

| Property | Description |
|---|---|
| Is there another web proxy on your network? | Is there another proxy on your network, such that<br>traffic must pass through it? it will be upstream of the Web Security Appliance ?<br>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. |
| 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, on page 22

## Network / Cloud Connector Settings

Need to confirm page name and 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 proxy, either **Connect directly** to the Internet, or **Drop requests**. |
| Cloud Web Security Authorization Scheme | Method for authorizing transactions:<br>• Web Security Appliance public-facing IPv4 address.<br>• Authorization key included with each transaction. You can generate an authorization key within the Cisco Cloud Web Security Portal. |

## Network / Network Interfaces and Wiring

The IP address, network mask, and host name to use to manage the Web Security Appliance and, by default, for proxy (data) traffic.

You can use the host name 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.

| Setting | Description |
|---|---|
| Ethernet Port | (Optional) Check **Use M1 port for management only** if you want to use a separate port for data traffic.<br>If you configure the M1 interface for management traffic only, you must configure the P1 interface for data traffic. You must also define different routes for management and data traffic. However, you can configure the P1 interface even when the M1 interface is used for both management and data traffic.<br>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. |
| IP Address / Netmask | The IP address and network mask to use when managing the Web Security Appliance on this network interface. |
| Hostname | The host name to use when managing the Web Security Appliance on this network interface. |

## Network / Layer 4 Traffic Monitor Wiring

| Property | Description |
|---|---|
| Layer-4 Traffic Monitor | The type of wired connections plugged into the "T" interfaces:<br>• **Duplex TAP.** The T1 port receives both incoming and outgoing traffic.<br>• **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).<br>Cisco recommends using Simplex when possible because it can increase performance and security. |

## 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.

| Property | Description |
|---|---|
| Default Gateway | The default gateway IP address to use for the traffic through the Management and Data interfaces. |

| Property | Description |
|---|---|
| Static Routes Table | Optional static routes for management and data traffic. Multiple routes can be added.<br>• **Name** – A name used to identify the static route.<br>• **Internal Network** – The IPv4 address for this route's destination on the network.<br>• **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. |

## Network / Transparent Connection Settings



**Note** 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.

| 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 | Specifies that the Web Security Appliance is connected to a version 2 WCCP-capable router.<br>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.<br>When you enable the standard service, you can also enable router security and enter a passphrase. The passphrase used here must be used all appliances and WCCP routers within the same service group.<br>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.<br>A dynamic service type allows you to define a custom ID, port numbers, and redirection and load balancing options. |

## Network /Administrative Settings

| Property | Description |
|---|---|
| Administrator Passphrase | The passphrase used to access the Web Security Appliance for administrative purposes. |

| Property | Description |
|---|---|
| Email System Alerts To | The email address to which the appliance sends systems alerts. |
| Send Email via SMTP Relay Host (optional) | The address and port for an SMTP relay host that AsyncOS can use to send system generated email messages.<br>If no SMTP relay host is defined, AsyncOS uses the mail servers listed in the MX record. |
| AutoSupport | Specifies whether the appliance sends system alerts and weekly status reports to Cisco Customer Support. |
| SensorBase Network Participation | Specifies whether to participate in the Cisco SensorBase Network. If you participate, you can configure Limited or Standard (full) participation. Default is Standard.<br>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. |

## Security / Security Settings

| 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.<br>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.<br>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. |

| Option | Description |
|---|---|
| Malware and Spyware Scanning | Specifies whether to enable malware and spyware scanning using Webroot, McAfee, or Sophos. The default setting is that all three options are enabled. Most security services will be automatically enabled/disabled to match the services normally available for cloud policies. Similarly, policy-related defaults will not be applicable. At least one scanning option must be enabled.<br>If any option is enabled, also choose whether to monitor or block detected malware. The default setting is to monitor malware.<br>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.<br>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, on page 22
- Creating Proxy Groups for Upstream Proxies, on page 22


## Upstream Proxies Task Overview

| Task | More Information |
|---|---|
| • Connect the external proxy upstream of the Cisco Web Security Appliance . | Connect the Appliance, on page 11. |
| • Create and configure a proxy group for the upstream proxy. | Creating Proxy Groups for Upstream Proxies, on page 22. |
| • Create a routing policy for the proxy group to manage which traffic is routed to the upstream proxy. | Create Policies to Control Internet Requests, on page 213 |

## Creating Proxy Groups for Upstream Proxies

### Procedure

**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.<br>**Note**<br>You can enter the same proxy server multiple times to allow unequal load distribution among the proxies in the proxy group. |
| **Load Balancing** | The strategy that the web proxy uses to load balance requests between multiple upstream proxies. Choose from:<br>• **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.<br>• **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.<br>• **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.<br>• **Round robin**. The Web Proxy cycles transactions equally among all proxies in the group in the listed order.<br>**Note**<br>The Load Balancing option is dimmed until two or more proxies have been defined. |
| **Failure Handling** | Specifies the default action to take if all proxies in this group fail. Choose from:<br>• **Connect directly.** Send the requests directly to their destination servers.<br>• **Drop requests.** Discard the requests without forwarding them. |

**Step 4** Submit and commit your changes.

### What to do next

- Creating a Policy , on page 219

# Network Interfaces

- IP Address Versions, on page 24
- Enabling or Changing Network Interfaces, on page 24

# 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, on page 24
- DNS Settings, on page 52

# 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

### Procedure

**Step 1** Choose **Network** > **Interfaces**.

**Step 2** Click **Edit Settings**.

**Step 3** Configure the Interface options.

| Option | Description |
|---|---|
| Interfaces | Modify or add new IPv4 or IPv6 Address, Netmask, and Hostname details for the M1, P1, or P2 interfaces as required.<br>• **M1** – AsyncOS requires an IPv4 address for the M1 (Management) port. 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.<br>• **P1** and **P2** – Use an IPv4 address, IPv6 address, or both for the Data ports. 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.<br>**Note**<br>If the Management and Data interfaces are all configured, each must be assigned IP addresses on different subnets.<br>**Note**<br>When split routing is enabled, the Management interface cannot communicate with the Smart Licensing Portal. To register the Web Security Appliance with the Smart Licensing Portal, choose a Data interface.<br>**Note**<br>When split routing is configured, Web Security Appliance uses the data interface to contact the external DLP server, and the management interface is restricted to only the management traffic. This results in all DLP traffic being considered as data traffic instead of management traffic while routing traffic to the DLP server.<br>For example, when there are two packet captures with P1 and M1 interfaces filtered by DLP addresses, the DLP traffic is found on both interfaces. It is because of the management interface that sends keepalive packets to the DLP servers and DLP traffic comes from data interfaces. |
| Separate Routing for Management Services | Check **Restrict M1 port to appliance management services only** to limit M1 to management traffic only, requiring use of a separate port for data traffic.<br>**Note**<br>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. |

| Option | Description |
|---|---|
| Appliance Management Services | Enable/disable use of, and specify a default port number for, the following network protocols:<br>• **FTP** – Disabled by default.<br>• **SSH**<br>• **HTTP**<br>• **HTTPS**<br>Also, you can enable/disable redirection of HTTP traffic to HTTPS. |

**Step 4** Submit and commit your changes.

### What to do next

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

**Related Topics**

- Connect the Appliance, on page 11.
- IP Address Versions, on page 24
- Configuring TCP/IP Traffic Routes, on page 39

# Network Interface Card Configuration

This topic contains the following sections:


- Media Settings on Ethernet Interfaces, on page 26
- Network Interface Card Pairing/Teaming, on page 27
- Enabling NIC Pairing using the etherconfig Command, on page 28
- Guidelines for Configuring NIC Pairing, on page 35


## Media Settings on Ethernet Interfaces

You can access the media settings for the ethernet interfaces using the **etherconfig** command. Each ethernet interface is listed with its current setting. By selecting the interface, the applicable media settings are displayed.

### Using etherconfig to Edit Media Settings on the Ethernet Interfaces

Use the **etherconfig** command to set the duplex settings (full/half) and the speed (10/100/1000 Mbps) of the ethernet interfaces. By default, interfaces automatically select the media settings; which you can override.

**Note** If you have completed the GUI's System Setup Wizard (or the Command Line Interface **systemsetup** command) as described in the Setup and Installation topic and committed the changes, the default ethernet interface settings should already be configured on your appliance.

### Example of Editing Media Settings

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
[]> MEDIA
Ethernet interfaces:
1. Management (Autoselect: <1000baseT full-duplex>) 00:50:56:87:a6:46
2. P1 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:1c:3f
3. P2 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:6a:42
4. T1 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:1c:3f
5. T2 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:fc:01

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>
```

## Network Interface Card Pairing/Teaming

NIC pairing allows you to combine any two physical data ports to provide a backup Ethernet interface if the data path from the NIC to the upstream Ethernet port should fail. Basically, pairing configures the Ethernet interfaces so that there is a primary interface and a backup interface. If the primary interface fails (for example, if the carrier between the NIC and the upstream node is disrupted), the backup interface becomes active and an alert is sent. When the primary interface become available, this interface automatically becomes active. Within the documentation for this product, NIC pairing is synonymous with NIC teaming.

**Note** NIC pairing is not available on S170, S190 and S195 web gateways.

You can create more than one NIC pair, provided you have enough data ports. When creating pairs, you can combine any two data ports. For example:

- Data 1 and Data 2
- Data 3 and Data 4
- Data 2 and Data 3

Some web gateways contain a fiber optic network interface option. If available, you will see two additional ethernet interfaces (Data 3 and Data 4) in the list of available interfaces on these web gateways. In a heterogeneous configuration, these gigabit fiber optic interfaces can be paired with the copper (Data 1, Data 2, and Management) interfaces.

Web Security Appliance does not support packet capture for the NIC paired interfaces. The packet capture will be applied only for the active interface. For example, if both P1 and P2 are paired, both P1 and P2 will not be configured in the user interface or the CLI.

### NIC Pairing and VLANs

VLANs (see Virtual Local Area Networks (VLANs)) are allowed only on the primary interface.

### NIC Pair Naming

When creating NIC pairs, you must specify a name for the pair. NIC pairs created in AsyncOS prior to version 4.5 will automatically receive the default name of 'Pair 1' following an upgrade.

Any alerts generated on NIC pairing will reference the specific NIC pair by its name.

### NIC Pairing and Existing Listeners

If you enable NIC pairing on an interface that has listeners assigned to it, you are prompted to either delete, reassign, or disable all listeners assigned to the backup interface.

## Enabling NIC Pairing using the etherconfig Command

**Note** NIC pairing is not available on S170, S190 and S195 web gateways.

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> PAIRING
Paired interfaces:
Choose the operation you want to perform:
- NEW - Create a new pairing.
[]> NEW
Please enter a name for this pair (Ex: "Pair 1"):
[]> DP1

1. P1
2. P2
Enter the name or number of the primary ethernet interface you wish bind to.
[]> 1

1. P2
2. T1
3. T2
Enter the name or number of the backup ethernet interface you wish to pair.
[]> 2

Paired interfaces:
1. DP1:
        Primary (P1)
        Backup (T1)

Choose the operation you want to perform:
- NEW - Create a new pairing.
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
```

```
- MTU - View and configure MTU.
[]>
example.com> commit
Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
Warning: Processing of network configuration changes might
cause a brief interruption in network availability.
Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Thu Sep 24 01:40:34 2020 MST
example.com> interfaceconfig


Currently configured interfaces:
1. Management (10.10.192.167/24 on Management: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]> NEW
Ethernet interface:
1. Management
2. DP1
3. P2
[1]> 2
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
IPv4 Address (Ex: 192.168.1.2 ):
[]> 10.10.102.66
Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 27
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
Hostname:
[]> example.com
Currently configured interfaces:
1. Management (10.10.192.167/24 on Management: example.com)
2. P1 (10.10.102.66/27 on DP1: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]>
example.com>example.com> commit
Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
Warning: Processing of network configuration changes might
cause a brief interruption in network availability.
Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Thu Sep 24 01:43:18 2020 MST
example.com> exitexample.com:rtestuser 53] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
```

```
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:fc:01
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet6 fe80::250:56ff:fe87:a646%lagg0 prefixlen 64 scopeid 0x7
        inet 10.10.102.66 netmask 0xfffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        groups: lagg
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
example.com:rtestuser 54]
```

## Bringing Down the P1 Interface

P1 and T1 are paired and named as DP1. By bringing P1 down, T1 will become active. In the following example, look for the lagg0 interface.

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
```

```
[]> PAIRING
Paired interfaces:
1. DP1:
        Backup (T1) Standby, Link is up
        Primary (P1) Active, Link is up
2. DP2:
        Backup (T2) Standby, Link is up
        Primary (P2) Active, Link is up

Choose the operation you want to perform:
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
example.com>
example.com> exit

example.com:rtestuser 115] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
```

```
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xfffffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xfffffffe0 broadcast 10.10.166.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 116]
example.com:rtestuser 116] ifconfig nic1 down
example.com:rtestuser 117] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
```

```
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xfffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=1<MASTER>
        laggport: nic3 flags=4<ACTIVE>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xfffffe0 broadcast 10.10.166.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 118]
```

## Bringing Up the P1 Interface

```
example.com:rtestuser 118] ifconfig nic1 up
example.com:rtestuser 119] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
```

```
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xfffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xfffffe0 broadcast 10.10.166.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 120]
example.com:rtestuser 120]
```

## Guidelines for Configuring NIC Pairing

M2, Data1, and Data2 cannot be used as primary or secondary or configured with an IP address.

***Table 3:***

| Ports | Configured as IP Address | Action | What to do? | Split Routing Enabled | |
|---|---|---|---|---|---|
| | | | | Primary | Secondary |
| P1 (Proxy) | Yes | Enabled | Connect P1 to the network for both incoming and outgoing traffic. | You can select P1 as primary for NIC Pairing<br>**Note** If you select P2 as primary then you must delete the IP address for the P1. | P2, T1, T2 |
| P1 + P2 (Proxy) | Yes | Enabled | Connect P1 to the internal network and P2 to the internet. | If you select P2 as primary and P1 as secondary, then you must delete the IP address for the P1.<br>You will be prompted during the NIC pairing to delete the IP. | T1, T2 |
| T1 (Traffic monitor) | No | Duplex Tap | One cable for all incoming and outgoing traffic. | NA | NA |
| T1 + T2 (Traffic monitor) | Yes | Simple Tap | One cable for all packets destined for the internet (T1) and one cable for all packets coming from the internet (T2). | NA | NA |

**Note** If you choose to delete the IP for P1, then P1 will not be configured under split routing. When IP address is assigned for P2 or for the created NIC pair, then Split routing is enabled with only P2 configured. Link Aggregation (LAGG) interface is not shown till IP address is not assigned to the primary (p2) or NIC pair. Once the IP address is assigned to the primary (p2) or the NIC pair, LAGG interface is created.

# Configuring Failover Groups for High Availability

Using the Common Address Redundancy Protocol (CARP), the Web Security Appliance enable multiple hosts on your network to share an IP address, providing IP redundancy to ensure high availability of services provided by those hosts.

Failover is available only for the proxy service. The proxy automatically binds to the failover interface when the failover group is created. Thus, if the proxy goes down for any reason, failover is triggered.

In CARP, there are three states for a host:

- primary - there can only be one primary host in each failover group
- backup
- init

The primary host in the CARP failover group sends regular advertisements to the local network so that the back-up hosts know it is still alive. (This advertisement interval is configurable on the Web Security Appliance ). If the back-up hosts do not receive an advertisement from the primary for the specified period of time (because the proxy is down, or the Web Security Appliance has gone down, or it is disconnected from the network), then failover is triggered and one of the backups will take over the duties of primary.

The advertisements from the primary Web Security Appliance do not reach the remaining back-up hosts in the following conditions:

- Network/Interface Unavailability
- OS Health and Availability



**Note** Disable Data-Plane IP Learning in the Application Centric Infrastructure (ACI) to use the Web Security Appliance High Availability feature.



**Note** You cannot use High Availability as a load balancing method between appliances. Use either WCCP or a hardware load balancer to load balance the traffic between devices.

The following are the configurations that causes high availability switchovers:

- Add or remove or update the Authentication Realm
- Add or remove or update the ISE settings
- Add or update the HTTPS certificate
- Update the log level ( proxy log )
- Update the transparent redirection setting
- Enable or disable or update the FTP proxy
- Enable or disable or update the SOCKS proxy

- Add or modify the PAC file
- Add or remove the interface from the appliance
- Add or update failover groups
- Enable or disable Upstream proxy
- Enable or disable WTT (web traffic tap)

# Add Failover Group

### Before you begin

- Identify a virtual IP address that will be used exclusively for this failover group. Clients will use this IP address to connect to the failover group in explicit forward proxy mode.
- Configure all Appliances in the failover group with identical values for the following parameters:
  - Failover Group ID
  - Hostname
  - Virtual IP Address
- If you are configuring this feature on a virtual appliance, ensure that the virtual switch and the virtual interfaces specific to each appliance are configured to use promiscuous mode. For more information, see the documentation for your virtual hypervisor.

### Procedure

**Step 1** Choose **Network > High Availability**.

**Step 2** Click **Add Failover Group**.

**Step 3** Enter a **Failover Group ID** in the range 1 to 255.

**Step 4** (Optional) Enter a Description.

**Step 5** Enter the **Hostname**, for example www.example.com.

**Step 6** Enter the **Virtual IP Address and Netmask**, for example 10.0.0.3/24 (IPv4) or 2001:420:80:1::5/32 (IPv6).

**Step 7** Choose an option from the **Interface** menu. The **Select Interface Automatically** option will select the interface based on the IP address you provided.

**Note**
If you do not select the **Select Interface Automatically** option, you must choose an interface in the same subnet as the virtual IP address you provided.

**Step 8** Choose the priority. Click **Primary** to set the priority to 255. Alternatively, select **Backup** and enter a priority between 1 (lowest) and 254 in the **Priority** field.

**Step 9** (Optional). To enable security for the service, select the **Enable Security for Service** check box and enter a string of characters that will be used as a shared secret in the **Shared Secret** and **Retype Shared Secret** fields.

**Note**

The shared secret, virtual IP, and failover group ID must be the same for all appliances in the failover group.

**Step 10** Enter the delay in seconds (1 to 255) between hosts advertising their availability in the **Advertisement Interval** field.

**Step 11** Submit and commit your changes.

### What to do next

### Related Topics

- Failover Problems, on page 559

## Edit High Availability Global Settings

### Procedure

**Step 1** Choose **Network > High Availability**.

**Step 2** In the **High Availability Global Settings** area, click **Edit Settings**.

**Step 3** In the **Failover Handling** menu, choose an option.

- **Preemptive**—The highest priority host will assume control when available.
- **Non-preemptive**—The host in control will remain in control even if a higher priority host becomes available.

**Step 4** Click **Submit**. Alternatively, click **Cancel** to abandon your changes.

## View Status of Failover Groups

Choose **Network > High Availability**. The Failover Groups area displays the current fail-over group. You can click **Refresh Status** to update the display. You can also view fail-over details by choosing **Network > Interfaces** or **Report > System Status**.

# 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.



**Note** 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.

### Before you begin

Enable P2 (you must also enable P1 if not already enabled) (see Enabling or Changing Network Interfaces, on page 24).

### Procedure

**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.

### What to do next

**Related Topics**

- Connect the Appliance, on page 11.
- Configuring TCP/IP Traffic Routes, on page 39.
- Configuring Transparent Redirection, on page 42

# Configuring TCP/IP Traffic Routes

Routes are used for determining where to send (or route) network traffic. The Web Security Appliance routes 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 types of traffic use the routes defined for all configured network interfaces. However, you can choose to split the routing, so that management traffic uses a management routing table and data traffic uses a data routing table. Both types of traffic split are split as follows:

| Management Traffic | Data Traffic |
|---|---|
| • WebUI<br>• SSH<br>• SNMP<br>• NTLM authentication (with domain controller)<br>• Syslogs<br>• FTP push<br>• DNS (configurable)<br>• Update/Upgrade/Feature Key (configurable) | • HTTP<br>• HTTPS<br>• FTP<br>• WCCP negotiation<br>• ICAP request with external DLP server<br>• DNS (configurable)<br>• Update/Upgrade/Feature Key (configurable)<br>• LDAP/NTLM authentication with domain controller (configurable) |

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 to appliance management services only** 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 not enabled). When you use the Management interface for both management and data traffic (**Restrict M1 port to appliance management services only** 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.

## Outbound Services Traffic

The Web Security Appliance  also uses the management and data interfaces to route outbound traffic for services such as DNS, software upgrades, NTP, and traceroute data traffic.You configure this for each service individually, by choosing the route it uses for outbound traffic. By default, the management interface is used for all services.

### Related Topics

- To enable split routing of management and data traffic, see Enabling or Changing Network Interfaces, on page 24.

## Modifying the Default Route

### Procedure

**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

### Procedure

**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

### Procedure

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

### Procedure

**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.

### What to do next

### Related Topics

- Enabling or Changing Network Interfaces, on page 24.

# Configuring Transparent Redirection


- Specifying a Transparent Redirection Device, on page 42
- Configuring WCCP Services, on page 43


## Specifying a Transparent Redirection Device

### Before you begin

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

### Procedure

**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: **Layer 4 Switch or No Device** or **WCCP v2 Router**.
**Step 4** Submit and commit your changes.
**Step 5** For WCCP v2 devices, complete these additional steps:
a) Configure the WCCP device using device documentation.
b) On the Web Security Appliance 's Transparent Redirection page, click **Add Service** to add a WCCP service, as described in Adding and Editing a WCCP Service, on page 45.
c) If IP spoofing is enabled on the appliance, create a second WCCP service.

### What to do next

### Related Topics

- Connect the Appliance, on page 11.
- Configuring WCCP Services, on page 43.

## Using An L4 Switch

If you are using a Layer 4 switch for transparent redirection, depending how it is configured, you may need to configure a few additional options on the Web Security Appliance .

- Generally, do not enable IP Spoofing; if you spoof upstream IP addresses you may create an asynchronous routing loop.
- On the Edit Web Proxy Settings page (Security Services > Web Proxy), check **Enable Identification of Client IP Addresses using X-Forwarded-For** in the **Use Received Headers** section (Advanced Settings). Then add one or more egress IP addresses to the **Trusted Downstream Proxy or Load Balancer** list.
- Optionally, you can use the CLI command `advancedproxyconfig` > `miscellaneous` to configure the following proxy-related parameters as necessary:
  - `Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)?` – Enter Y if you want to allow the Web Security Appliance to respond to health checks.
  - `Would you like proxy to perform dynamic adjustment of TCP receive window size?` – Use the default Y in most cases; enter N if you have another proxy device upstream of the Web Security Appliance .
  - `Do you want to pass HTTP X-Forwarded-For headers?` – No need unless there is a requirement upstream for X-Forwarded-For (XFF) headers.
  - `Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses?` – To aid in troubleshooting, you can enter Y; client IP addresses will be displayed in the access logs.
  - `Would you like the proxy to use client IP addresses from X-Forwarded-For headers?` Again, to aid policy configuration and reporting, you can enter Y.
- If you are using X-Forwarded-For (XFF) headers, add `%f` to the Access Logs subscription in order to log the XFF headers. For the W3C Logs format, add `cs(X-Forwarded-For)`.

## 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.

If WCCP proxy health checking is enabled, the Web Security Appliance 's WCCP daemon sends a proxy health check message (xmlrpc client request) to the xmlrpc server running on the Web proxy every 10 seconds. If the proxy is up and running, the WCCP service receives a response from the proxy and the Web Security Appliance sends a WCCP "here I am" (HIA) message to the specified WCCP-enabled routers every 10 seconds. If the WCCP service doesn't receive a reply from the proxy, then HIA messages are not sent to the WCCP routers.

After a WCCP router misses three consecutive HIA messages, the router removes the Web Security Appliance from its service group and traffic is no longer forwarded to the Web Security Appliance .

You can use the CLI command `advancedproxyconfig > miscellaneous > Do you want to enable WCCP proxy health check?` to enable and disable the proxy health check messages; the health check is disabled by default.

**Note** The WCCPv2 service works with the IPv4 and IPv6 networks. A maximum of 15 service groups can be configured on a single appliance. Each service group on the WCCP router can contain up to 32 appliances. The WCCPv2 service is also used for the Load Balancing mechanism to reduce content engine overloading and data blocking.

**Note** Configuring WCCP and High Availability on the same appliance is not supported. If configured, Web Security Appliance will not function as expected.


- About WCCP Load Balancing, on page 44
- Adding and Editing a WCCP Service, on page 45
- Creating WCCP Services for IP Spoofing, on page 47


## About WCCP Load Balancing

The **Assignment Weight** parameter in the WCCP service definition is used to adjust the load on this Web Security Appliance when it is operating as member of a WCCP pool, or service group. This weighting represents the proportion of total WCCP traffic that can be sent to this Web Security Appliance for processing.

Assignment weighting adjustment is required only when different types of gateway appliances are members of the same WCCP pool and you need to divert more of the traffic to the stronger appliances.

**Note** All Web Security Appliance s that are members of a WCCP pool must be running a version of AsyncOS that supports assignment weighting to benefit from WCCP load balancing.

**Note** WCCP load balances transparent traffic for up to 32 appliances. It balances the traffic flow based on hash or mask and they are weighted when several appliance models exist in the network. Without any downtime, you can add and remove devices from the service pool. However, if you are using or plan to use more than 8 appliances, we recommend having a dedicated load balancer.

See Adding and Editing a WCCP Service, on page 45 for more information about the **Assignment Weight** parameter.

## Adding and Editing a WCCP Service

### Before you begin

Configure the appliance to use a WCCP v2 Router (see Specifying a Transparent Redirection Device, on page 42).

### Procedure

**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:

| WCCP Service Option | Description |
|---|---|
| Service Profile Name | The name for the WCCP service.<br>**Note**<br>If you leave this empty and choose a standard service (see below), the name 'web_cache' is automatically assigned here. |
| Service | The service group type for the router. Choose from:<br>**Standard service.** This service type is assigned a fixed ID of zero, a fixed redirection method of *by destination port,* 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.<br>**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.<br>If you create a dynamic service, enter the following information:<br>• **Service ID.** You can enter any number from 0 to 255 in the Dynamic Service ID field. However, note that you can configure no more than 15 service groups on this appliance.<br>• **Port number(s).** Enter up to eight port numbers for traffic to redirect in the Port Numbers field.<br>• **Redirection basis.** Choose to redirect traffic based on the source or destination port. Default is destination port.<br>**Note**<br>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.<br>• **Load balancing basis.** When the network uses multiple Web Security Appliance , 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. |

| WCCP Service Option | Description |
|---|---|
| Router IP Addresses | 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. |
| Router Security | Check **Enable Security for Service** to require a passphrase for this service group. If enabled, every appliance and WCCP router that uses the service group must use the same passphrase.<br>Provide and confirm the passphrase to use. |
| Advanced | **Load-Balancing Method.** This determines how the router performs load balancing of packets among multiple Web Security Appliance . Choose from:<br>• **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. (IPv4 only.)<br>• **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. (IPv4 and IPv6.)<br>• **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.<br>**Mask Customization.** If you select Allow Mask Only or Allow Hash or Mask, you can customize the mask or specify the number of bits:<br>• **Custom mask (max 6 bits)**. You can specify the mask. The web interface displays the number of bits associated with the mask you provide. You can use up to five bits for an IPv4 router, or six bits for an IPv6 router.<br>• **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, between one and five bits.<br>**Assignment Weight** – The WCCP weighting for this Web Security Appliance ; valid values are zero to 255. This weighting represents the proportion of total traffic that can be sent to this Web Security Appliance for processing as member of a WCCP service group. A value of zero means this Web Security Appliance will be a part of the service group, but it will not receive any redirected traffic from the router. See About WCCP Load Balancing, on page 44 for more information.<br>**Forwarding method.** This is the method by which redirected packets are transported from the router to the web proxy.<br>**Return Method.** This is the method by which redirected packets are transported from the web proxy to the router. |

| WCCP Service Option | Description |
|---|---|
| | Both the forwarding and return methods use one of the following method types:<br>• **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 .<br>• **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.<br>• **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.<br>If the router is not directly connected to the appliance, you must choose GRE. |

**Step 4** Submit and commit your changes.

## Creating WCCP Services for IP Spoofing

### Procedure

**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).
- Configure spoofed IP addresses appropriately when you set WCCP load balancing methods **'Allow Mask Only'** or **'Allow Hash or Mask'** to distribute traffic to multiple appliances. Spoofed IP address configuration must ensure proper routing of traffic between the WCCP router and the Web Security Appliance .

### What to do next

### Related Topics

- Web Proxy Cache, on page 68.

# Increasing Interface Capacity Using VLANs

You can configure one or more VLANs to increase the number of networks the Cisco Web Security Appliance can connect to beyond the number of physical interfaces included.

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.

## 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.

**Note** Whenever you make changes to a VLAN configuration, ensure to reboot the appliance.

### Example 1: Creating a New VLAN

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

**Note** Do not create VLANs on the T1 or T2 interfaces.

### Procedure

**Step 1** 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.

### Procedure

**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.
- 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 "0xffffff00"):
[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.

### What to do next

**Related Topics**

- Enabling or Changing Network Interfaces, on page 24.
- Configuring TCP/IP Traffic Routes, on page 39.

# 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

### Procedure

**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

### Procedure

**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

### Procedure

**Step 1** Choose **Network > Internal SMTP Relay**.

**Step 2** Click **Edit Settings**.

**Step 3** Complete the Internal SMTP Relay settings.

| 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.

You can also specify secondary DNS name servers to resolve the queries not resolved by the primary name servers. Secondary DNS servers are not used as failover DNS servers. They are queried according to the priority, when primary DNS servers return errors specified in Editing DNS Settings, on page 53.

To prevent authentication failures, ensure that the Web Security Appliance  authentication redirect name is unique.


- Split DNS, on page 52
- Clearing the DNS Cache, on page 52
- Editing DNS Settings, on page 53


# 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.

**Procedure**

**Step 1** Choose **Network > DNS**.

**Step 2** Click **Clear DNS Cache**.

# Editing DNS Settings

**Procedure**

**Step 1** Choose **Network > DNS**

**Step 2** Click **Edit Settings**.

**Step 3** Configure the DNS settings as required.

| Property | Description |
|---|---|
| Primary DNS Servers | **Use these DNS Servers.** The local DNS server(s) that the appliance can use to resolve hostnames.<br>**Alternate DNS servers Overrides (Optional)**. Authoritative DNS servers for particular domains<br>**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.<br>**Note**<br>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. This is required for accessing the new web interface as well. |
| Secondary DNS Servers | The secondary DNS server(s) that the appliance can use to resolve hostnames not resolved by the primary name servers.<br>**Note**<br>The secondary DNS servers receive host name queries when the primary DNS servers return the following errors:<br>• No Error, no answer section received.<br>• Server failed to complete request, no answer section.<br>• Name Error, no answer section received.<br>• Function not implemented.<br>• Server Refused to Answer Query. |

| Property | Description |
|---|---|
| Routing Table for DNS Traffic | Specifies which interface the DNS service will route traffic through. |
| IP Address Version Preference | When a DNS server provides both an IPv4 and an IPv6 address, AsyncOS uses this preference to choose the IP address version.<br>**Note**<br>AsyncOS does not honor the version preference for transparent FTP requests. |
| 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.

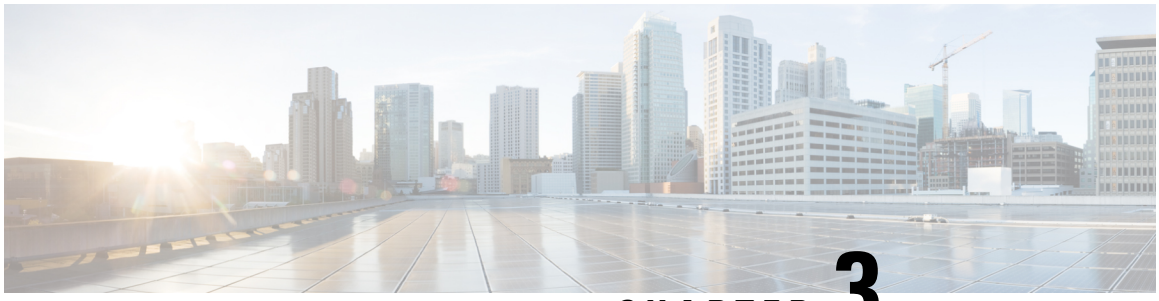
### What to do next

### Related Topics

- Configuring TCP/IP Traffic Routes, on page 39
- IP Address Versions, on page 24

# Troubleshooting Connect, Install, and Configure


- Failover Problems, on page 559
- Upstream Proxy Does Not Receive Basic Credentials, on page 579
- Client Requests Fail Upstream Proxy, on page 579
- Maximum Port Entries, on page 581



CHAPTER 3

# Connect the Appliance to a Cisco Cloud Web Security Proxy

This topic contains the following sections:


- How to Configure and Use Features in Cloud Connector Mode , on page 55
- Deployment in Cloud Connector Mode , on page 55
- Configuring the Cloud Connector, on page 56
- Controlling Web Access Using Directory Groups in the Cloud, on page 59
- Bypassing the Cloud Proxy Server, on page 59
- Partial Support for FTP and HTTPS in Cloud Connector Mode , on page 60
- Preventing Loss of Secure Data, on page 60
- Viewing Group and User Names and IP Addresses , on page 60
- Subscribing to Cloud Connector Logs, on page 60
- Identification Profiles and Authentication with Cloud Web Security Connector , on page 61


## How to Configure and Use Features in Cloud Connector Mode

Use of the features included in the Cloud Connector subset is the same as in standard mode, except as noted. See Comparison of Modes of Operation, on page 8 for additional information.

This topic links to locations within this documentation 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 document.

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

This document does not include information about the Cisco Cloud Web Security product. Cisco Cloud Web Security documentation is available from http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

## Deployment in Cloud Connector Mode

When you initially set up the appliance, you choose whether to deploy in Cloud Connector mode or standard mode. You can also run the System Setup Wizard on an appliance that is currently deployed in standard mode

to redeploy it in Cloud Connector mode, if you have the required licensing. Running the System Setup Wizard overwrites your existing configurations and deletes all existing data.

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.

To modify Cloud Connector settings after initial setup, select **Network** > **Cloud Connector**.

**Related Topics**

- Connect, Install, and Configure, on page 7

# Configuring the Cloud Connector

### Before you begin

See Enabling Access to the Web Interface on Virtual Appliances.

### Procedure

**Step 1** Access the Web Interface for the Web Security Appliance :

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** Select **System Administration > System Setup Wizard**.

**Step 3** Accept the terms of the license agreement.

**Step 4** Click **Begin Setup**.

**Step 5** 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.<br>See also DNS Settings, on page 52. |
| 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. |

**Step 6** Select **Cloud Web Security Connector** for the appliance mode.

**Step 7** 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 proxy, either **Connect directly** to the Internet or **Drop requests**. |
| Cloud Web Security Authorization Scheme | Method for authorizing transactions:<br>• Web Security Appliance public facing IPv4 address<br>• Authorization key included with each transaction. You can generate an authorization key within the Cisco Cloud Web Security Portal. |

**Step 8** 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. |

**Step 9** 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. |

**Step 10** Configure transparent connection settings:

**Note**
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<br>or<br>No Device | • The Web Security Appliance is connected to a layer 4 switch.<br>or<br>• 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.<br>Note: A passphrase can contain up to seven characters and is optional. |

**Step 11** Configure administrative settings:

| Setting | Description |
|---|---|
| Administrator Passphrase | A passphrase to access the Web Security Appliance . The passphrase 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.<br>The default SMTP relay host is the mail servers listed in the MX record.<br>The default port number is 25. |
| AutoSupport | The appliance can send system alerts and weekly status report to Cisco Customer Support. |

**Step 12** Review and install:

a) Review the installation.
b) Click **Previous** to go back and make changes.
c) Click **Install This Configuration** to continue with the information you provided.

### What to do next

**Related Topics**

- Preventing Loss of Secure Data, on page 60
- Network Interfaces, on page 23
- Configuring TCP/IP Traffic Routes, on page 39
- Configuring Transparent Redirection, on page 42
- Managing Alerts, on page 518
- Configuring an SMTP Relay Host, on page 51

# Controlling Web Access Using Directory Groups 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.

### Before you begin

Add an authentication realm to the Web Security Appliance configuration.

### Procedure

**Step 1** Navigate to **Network** > **Cloud Connector**.

**Step 2** In the **Cloud Policy Directory Groups** area, click **Edit Groups**.

**Step 3** Select the User Groups and Machine 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.

### What to do next

### Related information

- Authentication Realms, on page 99

# Bypassing the Cloud Proxy Server

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

- **Identification Profile**
- 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 , on page 219

# Partial Support for FTP and HTTPS in Cloud Connector Mode

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

### 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 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

- Prevent Loss of Sensitive Data, on page 313

# Viewing Group and User Names and IP Addresses

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

# Subscribing to 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.

### Procedure

**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.

### What to do next

**Related Topics**

- Monitor System Activity Through Logs, on page 425

# Identification Profiles and Authentication with Cloud Web Security Connector

The Cloud Web Security Connector supports basic authentication and NTLM. You can also bypass authentication for certain destinations.

In Cloud Connector mode, using an Active Directory realm, you can identify transaction requests as originating from specific machines. The Machine ID service is not available in standard mode.

With two exceptions, Authentication works the same throughout the Web Security Appliance , whether in standard configuration or Cloud Connector configuration. Exceptions:

- The Machine ID service is not available in standard mode.
- AsyncOS does not support Kerberos when the appliance is configured in Cloud Connector mode.



**Note** Identification Profiles based on User Agent or Destination URL are not supported for HTTPS traffic.

**Related Topics**

- Identifying Machines for Policy Application, on page 62
- Guest Access for Unauthenticated Users, on page 62
- Classify End-Users for Policy Application, on page 129
- Overview of Acquire End-User Credentials, on page 87

# Identifying Machines for Policy Application

By enabling the Machine ID service, AsyncOS can apply policies based on the machine that made the transaction request rather than the authenticated user or IP address or some other identifier. AsyncOS uses NetBIOS to acquire the machine ID.

**Note** Be aware that the machine identity service is only available through Active Directory realms. If you do not have an Active Directory realm configured, this service is disabled.

### Procedure

**Step 1** Select **Network > Machine ID Service**.

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

**Step 3** Configure Machine Identification settings:

| Setting | Description |
|---|---|
| Enable NetBIOS for Machine Identification | Select to enable the machine identification service. |
| Realm | The Active Directory realm to use to identify the machine that is initiating the transaction request. |
| Failure Handling | If AsyncOS cannot identify the machine, should it drop the transaction or continue with policy matching? |

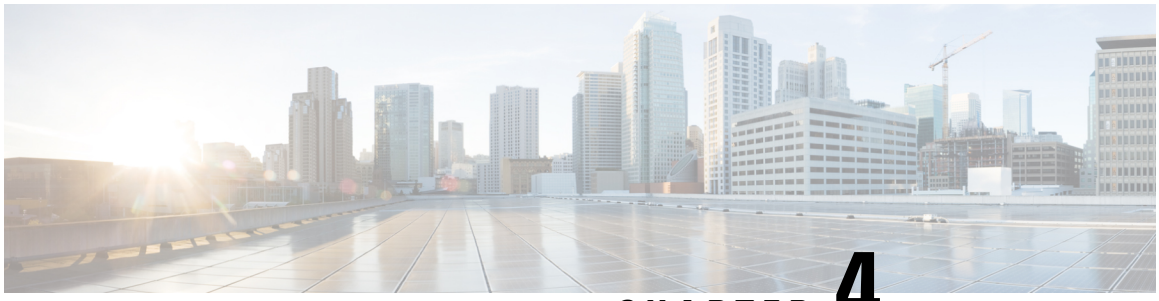
**Step 4** Submit and Commit your changes.

# 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, on page 122



CHAPTER 4

# Intercepting Web Requests

This topic contains the following sections:


- Overview of Intercepting Web Requests, on page 63
- Tasks for Intercepting Web Requests, on page 63
- Best Practices for Intercepting Web Requests, on page 64
- Web Proxy Options for Intercepting Web Requests, on page 65
- Domain Map, on page 75
- Client Options for Redirecting Web Requests, on page 77
- Using PAC Files with Client Applications, on page 77
- FTP Proxy Services, on page 80
- SOCKS Proxy Services, on page 82
- Troubleshooting Intercepting Requests, on page 85


## 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 Appliance s.

## Tasks for Intercepting Web Requests

| Steps | Task | Links to Related Topics and Procedures |
|---|---|---|
| Step 1 | Review best practices. | • Best Practices for Intercepting Web Requests, on page 64 |

| Steps | Task | Links to Related Topics and Procedures |
|---|---|---|
| Step 2 | (Optional) Perform follow up networking tasks:<br>• Connect and configure upstream proxies.<br>• Configure network interface ports.<br>• Configure transparent redirection devices.<br>• Configure TCP/IP routes.<br>• Configure VLANs. | • Upstream Proxies, on page 22<br>• Network Interfaces, on page 23<br>• Configuring Transparent Redirection, on page 42<br>• Configuring TCP/IP Traffic Routes, on page 39<br>• Increasing Interface Capacity Using VLANs, on page 48 |
| Step 3 | (Optional) Perform follow up Web Proxy tasks:<br>• Configure the web proxy to operate in either Forward or Transparent mode.<br>• Decide if additional services are needed for the protocol types you want to intercept<br>• Configure IP spoofing.<br>• Manage the web proxy cache.<br>• Use custom web request headers.<br>• Bypass the proxy for some requests. | • Web Proxy Options for Intercepting Web Requests, on page 65<br>• Configuring Web Proxy Settings, on page 65<br>• Web Proxy Options for Intercepting Web Requests, on page 65<br>• Web Proxy Cache, on page 68<br>• Web Proxy IP Spoofing, on page 70<br>• Web Proxy Bypassing, on page 73 |
| Step 4 | Perform client tasks:<br>• Decide how clients should redirect requests to the web proxy.<br>• Configure clients and client resources. | • Client Options for Redirecting Web Requests, on page 77<br>• Using PAC Files with Client Applications, on page 77 |
| Step 5 | (Optional) Enable and Configure the FTP proxy. | • FTP Proxy Services, on page 80 |

# 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, on page 80
- SOCKS Proxy Services, on page 82

# Configuring Web Proxy Settings

### Before you begin

Enable the web proxy.

### Procedure

**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.<br>The web proxy caches data to increase performance. |

| Property | Description |
|---|---|
| Proxy 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.<br>• **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. |
| IP Spoofing Connection Type | If you have selected the Proxy Mode as **Transparent**, choose one of the IP spoofing connection types:<br>• **For Transparent Connections Only** - To configure IP Spoofing for transparent connections only.<br>• **For All Connections** - To configure IP Spoofing for Transparent and Explicit connections.<br>If you have selected the Proxy Mode as **Forward**, then the IP Spoofing Connection Type is always Explicit.<br>**Note**<br>The IP spoofing connection type that you choose is applicable for all protocols - native FTP, HTTP, and HTTPS.<br>To add IP spoofing profiles in routing policies, see Adding Routing Destination and IP Spoofing Profile to Routing Policy, on page 223 |

**Step 4** Complete the advanced web proxy settings as required.

| Property | Description |
|---|---|
| Persistent Connection Timeout | 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.<br>• **Client side.** The timeout value for connections to clients.<br>• **Server side.** The timeout value for connections to servers.<br>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.<br>Cisco recommends keeping the default values. |
| In-Use Connection Timeout | 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.<br>• **Client side.** The timeout value for connections to clients.<br>• **Server side.** The timeout value for connections to servers. |

| Property | Description |
|---|---|
| Simultaneous Persistent Connections (Server Maximum Number) | The maximum number of connections (sockets) the Web Proxy keeps open with servers. |
| Generate Headers | Generate and add headers that encode information about the request.<br>• **X-Forwarded-For** headers encode the IP address of the client from which an HTTP request originated.<br>**Note**<br>• To turn header forwarding on or off, use the CLI `advancedproxyconfig` command, Miscellaneous option, "Do you want to pass HTTP X-Forwarded-For headers?"<br>• Using an explicit forward upstream proxy to manage user authentication or access control with proxy authentication requires forwarding of these headers.<br>• For transparent HTTPS requests, the appliance does not decrypt the XFF header. For explicit requests, the appliance uses the XFF header received in the CONNECT request, and does not decrypt the XFF inside the SSL tunnel, so identification of client IP Addresses using X-Forwarded-For is not applicable for HTTPS transparent requests.<br>• **Request Side VIA** headers encode the proxies through which the request passed on its way from the client to the server.<br>• **Response Side VIA** headers encode the proxies through which the request passed on its way from the server to the client. |
| Use Received Headers | 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.<br>If enabled, requires the IP address of a downstream proxy or load balancer (you cannot enter subnets or host names). |
| Range Request Forwarding | Use the **Enable Range Request Forwarding** check box to enable or disable forwarding of range requests. Refer to Managing Access to Web Applications, on page 303 for more information. |

**Step 5** Submit and commit your changes.

### What to do next

- Web Proxy Cache, on page 68
- Configuring Transparent Redirection, on page 42

# Web Proxy Cache

The web proxy caches data to increase performance. AsyncOS includes defined caching modes that range from safe to aggressive, and also allows customized 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

### Procedure

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

**Step 2** Click **Clear Cache** and confirm your action.

## Removing URLs from the Web Proxy Cache

### Procedure

**Step 1** Access the CLI.

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

```
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
[]> 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 Caches

### Procedure

**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** Enter **add** to add new entries:

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

**Step 5** Enter domains or URLs, one per line; 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
[]>
```

You can include certain regular expression (regex) characters when specifying a domain or URLs. With the `DOMAINS` option, you can use a preceding dot character to exempt an entire domain and its subdomains from caching. For example, you can enter `.google.com` rather than simply `google.com` to exempt www.google.com, docs.google.com, and so on.

With the `URLS` option, you can use the full suite of regular-expression characters. See Regular Expressions, on page 195 for more information about using regular expressions.

**Step 6** When you are finished entering values, press Enter until you are returned to the main command-line interface.

**Step 7** Commit your changes.

## Choosing The Web Proxy Cache Mode

### Procedure

**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.

### What to do next

### Related Topics

- Web Proxy Cache, on page 68.

# 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 appear to originate from client IP or any other routable custom IP address rather than from the Web Security Appliance . You can configure Web Proxy IP Spoofing by creating IP spoofing profiles for custom IP addresses and adding them to the routing policies.

IP spoofing works for transparent and explicitly forwarded traffic. When the Web Proxy is deployed in transparent mode, you can configure the IP Spoofing Connection Type 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.

IP spoofing profiles have a limitation when the HTTPS traffic is transparently redirected. See Accessing HTTPS Sites Using Routing Policies with URL Category Criteria, on page 563.

### Related Topics

- Creating IP Spoofing Profiles, on page 71
- Configuring Web Proxy Settings, on page 65
- Configuring WCCP Services, on page 43

## Creating IP Spoofing Profiles

### Before you begin

Make sure that you have selected the proxy mode and IP spoofing connection type in the web proxy settings. For more information, see Configuring Web Proxy Settings, on page 65.

### Procedure

**Step 1** Choose **Web Security Manager** > **IP Spoofing Profiles**.

**Step 2** Click **Add Profile**.

**Step 3** Enter a name for the IP spoofing profile.

**Step 4** Enter the IP address that you want to assign to the spoofing profile name.

**Step 5** Submit and commit your changes.

### What to do next

Add the IP spoofing profile to a routing policy. For more information, see Adding Routing Destination and IP Spoofing Profile to Routing Policy, on page 223.

### Related Topics

Editing IP Spoofing Profiles, on page 72
Deleting IP Spoofing Profiles, on page 72

### Editing IP Spoofing Profiles



**Note** Once you update an IP spoofing profile, it will be updated in all the routing policies associated with that profile.

#### Procedure

**Step 1** Choose **Web Security Manager** > **IP Spoofing Profiles**.

**Step 2** Click the IP spoofing profile name link that you want to edit.

**Step 3** Modify the profile details.

**Step 4** Submit and commit your changes.

### Deleting IP Spoofing Profiles

#### Procedure

**Step 1** Choose **Web Security Manager** > **IP Spoofing Profiles**.

**Step 2** Click the trash can icon corresponding to the IP spoofing profile that you want to delete.

**Note**
The appliance displays a warning if the IP spoofing profile that you are deleting is assigned to one or more routing policies. In this case, select a different IP spoofing profile to be assigned to all those affected routing policies.

**Step 3** Submit and commit your changes.

# 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

#### Procedure

**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.<br>Example header:<br>X-YouTube-Edu-Filter: ABCD1234567890abcdef<br>(The value in this case is a unique key provided by YouTube.)<br>Example domain:<br>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, on page 73
- Configuring Web Proxy Bypassing for Web Requests, on page 74
- Configuring Web Proxy Bypassing for Applications, on page 74


## 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

### Procedure

**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.

**Note**
When you configure /0 as a subnet mask for any IP in the bypass list, the appliance bypasses all the web traffic. In this case, the appliance interprets the configuration as 0.0.0.0/0.

**Step 4** Choose the Custom URL Categories that you want to add to the proxy bypass list.

**Note**
You cannot set the web proxy bypass for Regular Expressions.

**Note**
Once you add the Custom URL Categories to the proxy bypass list, all the IP addresses and the domain names of the Custom URL categories are bypassed for both the source and destination.

**Step 5** Submit and commit your changes.

## Configuring Web Proxy Bypassing for Applications

### Procedure

**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.

**Note**

Webex bypass settings are only applicable to HTTPS traffic. However, for HTTP traffic the applications can be blocked via Access Policies.

## 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, on page 327

# Domain Map

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

You can use passthrough for applications that require traffic to pass through the appliance, without undergoing any modification, or certificate checks of the destination servers.

## Domain Map for Specific Applications

**Before you begin**

Ensure you have an identification policy defined for the devices that require pass through traffic to specific servers. See Classifying Users and Client Software, on page 131 for more information. Specifically, you must:

- Choose **Exempt from authentication/identification**.
- Specify the addresses to which this Identification Profile should apply. You can use IP addresses, CIDR blocks, and subnets.

**Procedure**

**Step 1** Enable HTTPS Proxy. See Enabling the HTTPS Proxy, on page 245 for more information.

**Step 2** Choose **Web Security Manager** > **Domain Map**.

a) Click **Add Domain**.
b) Enter the **Domain Name** or the destination server.
c) Choose the order of the priority if there are existing domains specified.
d) Enter the IP addresses.
e) Click **Submit**.

**Step 3** Choose **Web Security Manager** > **Custom and External URL Categories**.

a) Click **Add Category**.
b) Provide the following information.

| Setting | Description |
|---|---|
| Category Name | Enter an identifier for this URL category. This name appears when you configure URL filtering for policy groups. |
| List Order | Specify the order of this category in the list of custom URL categories. Enter "1" for the first URL category in the list.<br>The URL filtering engine evaluates a client request against the custom URL categories in the order specified. |
| Category Type | Choose **Local Custom Category**. |
| Advanced | You can enter regular expressions in this section to specify additional sets of addresses.<br>You can use regular expressions to specify multiple addresses that match the patterns you enter.<br>See Regular Expressions, on page 195 for more information about using regular expressions. |

c) Submit and commit the changes.

**Step 4** Choose **Web Security Manager** > **Decryption Policies**.

a) Create a new decryption policy.
b) Choose the identification profile that you created for bypassing HTTPS traffic for specific applications.
c) In the **Advanced** panel, click the link for URL Categories.
d) In the **Add** column, click to add the custom URL category created in step 3.
e) Click **Done**.
f) In the Decryption Policies page, click the link for **URL Filtering**.
g) Choose **Pass Through**.
h) Submit and commit the changes.

You can use the **%(** format specifier to view access log information. See Customizing Access Logs, on page 460 for more information.

**Note**

- The Domain Map feature works in HTTPS Transparent mode.
- This feature does not work in Explicit mode and for HTTP traffic.
- Local Custom Category must be configured to allow the traffic using this feature.
- Enabling this feature will modify or assign the server name as per the server name configured in the Domain Map, even if SNI information is available.
- This feature does not block traffic based on domain name if that traffic matches the Domain Map and corresponding custom category, decryption policy and passthrough action are configured.
- Authentication does not work with this pass through feature. Authentication requires decryption, but traffic will not be decrypted in this case.
- UDP traffic is not monitored. You must configure UDP traffic not to come to the Web Security Appliance , instead it should go directly through firewall to the internet for applications like WhatsApp, Telegram etc.

- WhatsApp, Telegram and Skype works in Transparent mode. However, some apps like WhatsApp do not work in Explicit mode due to restrictions on the app.

# 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, on page 77

# 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 Appliance** .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 , on page 78
- Specifying PAC Files in Client Applications, on page 79
- Hosting PAC Files on the Web Security Appliance , on page 78
- Specifying PAC Files in Client Applications, on page 79

# 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, on page 80

# Hosting PAC Files on the Web Security Appliance

**Procedure**

**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 hostnamevalue. |
| 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.<br>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, on page 79
- Detecting the PAC File Automatically in Clients, on page 80


## Configuring a PAC File Location Manually in Clients

### Procedure

**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.

### What to do next


- Hosting PAC Files on the Web Security Appliance , on page 78

## Detecting the PAC File Automatically in Clients

### Procedure

**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.

### What to do next

- Using PAC Files with Client Applications, on page 77
- Hosting PAC Files on the Web Security Appliance , on page 78
- WPAD Not Working With Firefox, on page 559

# FTP Proxy Services


- Overview of FTP Proxy Services, on page 80
- Enabling and Configuring the FTP Proxy, on page 81


## 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, on page 81
- Configuring FTP Notification Messages, on page 336

# Enabling and Configuring the FTP Proxy

**Note** To configure proxy settings that apply to FTP over HTTP connections, see Configuring Web Proxy Settings, on page 65.

## Procedure

**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 of not data connections from anonymous users are cached.<br>**Note**<br>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. |
| Client IP Spoofing | Allows the FTP Proxy to imitate the FTP client's source IP address. When enabled, the FTP requests appear to originate from the FTP client rather than the FTP Proxy. |
| 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.<br>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 *same* FTP server immediately after being used. As a result, any given FTP server cannot connect to the FTP Proxy in active mode more than *n* times in a short period of time, where *n* is the number of ports specified in this field. |

| Property | Description |
|---|---|
| Welcome Banner | The welcome banner that appears in FTP clients during connection. Choose from:<br>• **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.<br>• **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 | 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.<br>• **Client side.** The timeout value for control connections to idle FTP clients.<br>• **Server side.** The timeout value for control connections to idle FTP servers. |
| Data Connection Timeouts | 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.<br>• **Client side.** The timeout value for data connections to idle FTP clients.<br>• **Server side.** The timeout value for data connections to idle FTP servers. |

**Step 5** Submit and commit your changes.

### What to do next

- Overview of FTP Proxy Services, on page 80

# SOCKS Proxy Services


- Overview of SOCKS Proxy Services, on page 82
- Enabling Processing of SOCKS Traffic, on page 83
- Configuring the SOCKS Proxy, on page 83
- Creating SOCKS Policies, on page 84


## 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 that control SOCKS traffic. Similar to access policies, you can make use of Identification Profiles to specify which transactions are governed by each SOCKS policy. Once SOCKS policies are applied to transactions, routing policies can then govern routing of the traffic.

Note the following regarding the SOCKS proxy:

- The SOCKS protocol only supports direct forward connections.
- The SOCKS proxy does not support (will not forward to) upstream proxies.
- The SOCKS proxy does not support scanning services, which are used by Application Visibility and Control (AVC), Data Loss Prevention (DLP), and malware detection.
- The SOCKS proxy does not support policy tracing.
- The SOCKS proxy does not decrypt SSL traffic; it tunnels from client to server.

# Enabling Processing of SOCKS Traffic

### Before you begin

Enable the Web Proxy.

### Procedure

**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

### Procedure

**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.

| | |
|---|---|
| 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

### Procedure

**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.

| | |
|---|---|
| Proxy Ports | The port configured in the browser.<br>(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.<br>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.<br>**Note**<br>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. |
| Subnets | (Optional) Define policy group membership by subnet or other addresses.<br>You can choose to use the **addresses** that may be **defined** with the associated **Identity**, or you can enter **specific addresses** here.<br>**Note**<br>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. |

| | |
|---|---|
| Time Range | (Optional) Define policy group membership by time range:<br>**a.** Select a time range from the **Time Range** field.<br>**b.** Specify whether this policy group should apply to the times inside or outside the selected time range. |

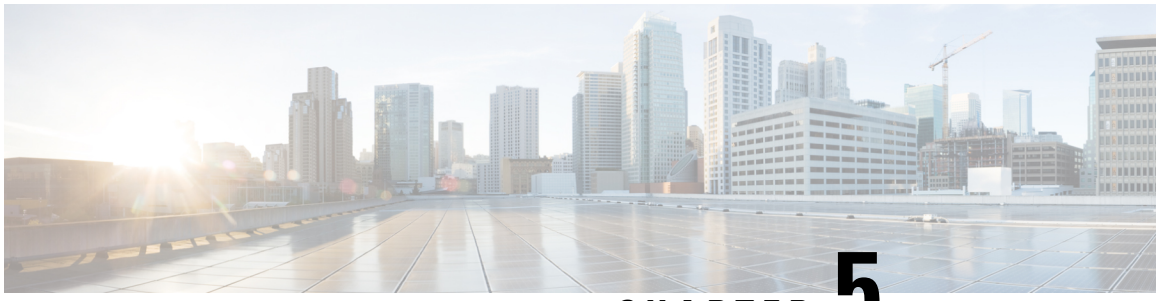
**Step 8** Submit and Commit Changes.

### What to do next

- (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, on page 560
- Large FTP Transfers Disconnect, on page 561
- Zero Byte File Appears On FTP Servers After File Upload, on page 561
- Unable to Route FTP Requests Via an Upstream Proxy, on page 580
- HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 572
- User Matches Global Policy for HTTPS and FTP over HTTP Requests, on page 573



CHAPTER 5

# Acquire End-User Credentials

This topic contains the following sections:


- Overview of Acquire End-User Credentials, on page 87
- Authentication Best Practices, on page 88
- Authentication Planning, on page 89
- Authentication Realms, on page 99
- Authentication Sequences, on page 117
- Failed Authentication, on page 119
- Credentials, on page 126
- Troubleshooting Authentication, on page 128


# Overview of Acquire End-User Credentials

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

## Authentication Task Overview

| Step | Task | Links to Related Topics and Procedures |
|---|---|---|
| 1 | Create an authentication realm. | • How to Create an Active Directory Authentication Realm (NTLMSSP and Basic), on page 104<br>• Creating an LDAP Authentication Realm, on page 107 |

| Step | Task | Links to Related Topics and Procedures |
|---|---|---|
| 2 | Configure global authentication settings. | • Configuring Global Authentication Settings, on page 112 |
| 3 | Configure external authentication.<br>You can authenticate users through an external LDAP or RADIUS server. | • External Authentication, on page 100 |
| 4 | (Optional) Create and order additional authentication realms.<br>Create at least one authentication realm for each authentication protocol and scheme combination you plan to use. | • Creating Authentication Sequences, on page 118 |
| 5 | (Optional) Configure credential encryption. | • Configuring Credential Encryption, on page 128 |
| 6 | Create Identification Profiles to classify users and client software based on authentication requirements. | • Classifying Users and Client Software, on page 131 |
| 7 | Create policies to manage Web requests from the users and user groups for which you created Identification Profiles. | • Managing Web Requests Through Policies Best Practices, on page 215 |

# 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.
- Some user agents are known to have issues with machine credentials or authentication failures, which can negatively impact normal operations. You should bypass authentication with these user agents. See Bypassing Authentication with Problematic User Agents , on page 120.
- Actively authenticating a client is a resource-intensive task. Authentication surrogates can be used to improve authentication performance by remembering an authenticated user for a set duration (default is 3600 seconds and configurable under (**Global Authentication** > **Surrogate Timeout**) after authentication has completed. IP surrogates should be used whenever possible to limit the number of active authentication events.
- For authentication setups with trusted Active Directory (AD), the authentication fails if the DC resolutions for the trusted domain is not successful. This is because of the introduction Samba 4.11.15, and it requires the trusted domain lookups to be successful. If the DC name resolution continues to fail, you must navigate

to **Network** > **Authentication** > **Authentication Server and Type and Scheme(s)** and uncheck the **Enable Trusted Domain Health Check** check box.

# Authentication Planning


- Active Directory/Kerberos, on page 89
- Active Directory/Basic, on page 90
- Active Directory/NTLMSSP, on page 91
- LDAP/Basic, on page 91
- Identifying Users Transparently, on page 92


## Active Directory/Kerberos

| Explicit Forward | Transparent, IP-Based Caching | Transparent, Cookie-Based Caching |
|---|---|---|
| **Advantages:**<br>• Better performance and interoperability when compared to NTLM<br>• Works with both Windows and non-Windows clients that have joined the domain<br>• Supported by all browsers and most other applications<br>• RFC-based<br>• Minimal overhead (Reauthentication is not required)<br>• Works for HTTPS (CONNECT) requests<br>• Because the passphrase is not transmitted to the authentication server, it is more secure<br>• Connection is authenticated, not the host or IP address<br>• Achieves true single sign-on in an Active Directory environment when the client applications are configured to trust the Web Security Appliance | **Advantages:**<br>• Better performance and interoperability when compared to NTLM<br>• Works with both Windows and non-Windows clients that have joined the domain<br>• Works with all major browsers<br>• With user agents that do not support authentication, users only need to authenticate first in a supported browser<br>• Relatively low overhead<br>• Works for HTTPS requests if the user has previously authenticated with an HTTP request | **Advantages**:<br>• Better performance and interoperability when compared to NTLM<br>• Works with both Windows and non-Windows clients that have joined the domain<br>• Works with all major browsers<br>• Authentication is associated with the user rather than the host or IP address<br>**Disadvantages**:<br>• Each new web domain requires the entire authentication process because cookies are domain specific<br>• Requires cookies to be enabled<br>• Does not work for HTTPS requests |

# Active Directory/Basic

| Explicit Forward | Transparent, IP-Based Caching | Transparent, Cookie-Based Caching |
|---|---|---|
| **Advantages:**<br>• Supported by all browsers and most other applications<br>• RFC-based<br>• Minimal overhead<br>• Works for HTTPS (CONNECT) requests<br>• Because the passphrase is not transmitted to the authentication server, it is more secure<br>• Connection is authenticated, not the host or IP address<br>• Achieves true single sign-on in an Active Directory environment when the client applications are configured to trust the Web Security Appliance<br>**Disadvantages**:<br>• Passphrase sent as clear text (Base64) for every request<br>• No single sign-on<br>• Moderate overhead: each new connection needs to be re-authenticated<br>• Primarily supported on Windows only and with major browsers only | **Advantages:**<br>• Works with all major browsers<br>• With user agents that do not support authentication, users only need to authenticate first in a supported browser<br>• Relatively low overhead<br>• Works for HTTPS requests if the user has previously authenticated with an HTTP request<br>**Disadvantages**:<br>• Authentication credentials are associated with the IP address, not the user (does not work in Citrix and RDP environments, or if the user changes IP address)<br>• No single sign-on<br>• Passphrase is sent as clear text (Base64) | **Advantages**:<br>• Works with all major browsers<br>• Authentication is associated with the user rather than the host or IP address<br>**Disadvantages**:<br>• Each new web domain requires the entire authentication process because cookies are domain specific<br>• Requires cookies to be enabled<br>• Does not work for HTTPS requests<br>• No single sign-on<br>• Passphrase is sent as clear text (Base64) |

# Active Directory/NTLMSSP

| Explicit Forward | Transparent |
|---|---|
| **Advantages:**<br>• Because the passphrase is not transmitted to the authentication server, it is more secure<br>• Connection is authenticated, not the host or IP address<br>• Achieves true single sign-on in an Active Directory environment when the client applications are configured to trust the Web Security Appliance<br>**Disadvantages:**<br>• Moderate overhead: each new connection needs to be re-authenticated<br>• Primarily supported on Windows only and with major browsers only | **Advantages:**<br>• More Flexible<br>Transparent NTLMSSP authentication is similar to transparent Basic authentication except that the Web Proxy communicates with clients using challenge and response instead of basic clear text username and passphrase.<br>The advantages and disadvantages of using transparent NTLM authentication are the same as those of using transparent Basic authentication except that transparent NTLM authentication has the added advantaged of not sending the passphrase to the authentication server and you can achieve single sign-on when the client applications are configured to trust the Web Security Appliance . |

# LDAP/Basic

| Explicit Forward | Transparent |
|---|---|
| **Advantages:**<br>• RFC-based<br>• More browser support than NTLM<br>• Minimal overhead<br>• Works for HTTPS (CONNECT) requests<br>**Disadvantages:**<br>• No single sign-on<br>• Passphrase sent as clear text (Base64) for every request<br>**Workarounds:**<br>• Failed Authentication, on page 119 | **Advantages:**<br>• More Flexible than explicit forward.<br>• More browser support than NTLM<br>• With user agents that do not support authentication, users only need to authenticate first in a supported browser<br>• Relatively low overhead<br>• Works for HTTPS requests if the user has previously authenticated with an HTTP request<br>**Disadvantages:**<br>• No single sign-on<br>• Passphrase is sent as clear text (Base64)<br>• Authentication credentials are associated with the IP address, not the user (does not work in Citrix and RDP environments, or if the user changes IP address)<br>**Workarounds:**<br>• Failed Authentication, on page 119 |

# Identifying Users Transparently

Traditionally, users are identified and authenticated by prompting them to enter a user name and passphrase. These credentials are validated against an authentication server, and then the Web Proxy applies the appropriate policies to the transaction based on the authenticated user name.

However, you can configure the Web Security Appliance to authenticate users transparently—that is, without prompting the end user for credentials. Transparent identification authenticates the user by means of credentials obtained from another trusted source, with the assumption that the user has already been authenticated by that trusted source, and then applies the appropriate policies.

You might want to identify users transparently to:

- Create a single sign-on environment so users are not aware of the presence of a proxy on the network.
- To apply authentication-based policies to transactions coming from client applications that are incapable of displaying an authentication prompt to end users.

Identifying users transparently only affects how the Web Proxy obtains the user name and assigns an Identification Profile. After it obtains the user name and assigns an Identification Profile, it applies all other policies normally, regardless of how it assigned the Identification Profile.

If transparent authentication fails, you can configure how to handle the transaction: you can grant the user guest access, or you can force an authentication prompt to appear to the user.

When an end user is shown an authentication prompt due to failed transparent user identification, and the user then fails authentication due to invalid credentials, you can choose whether to allow the user guest access.



**Note** When you enable re-authentication and a transaction is blocked by URL filtering, an end-user notification page appears with the option to log in as a different user. Users who click the link are prompted for authentication. For more information, see Failed Authorization: Allowing Re-Authentication with Different Credentials, on page 124.

## Understanding Transparent User Identification

The available methods of transparent user identification are:

- **Transparently identify users with ISE** – Available when the Identity Services Engine (ISE) or Passive Identity Connector (ISE-PIC) service is enabled (Network > Identity Services Engine). For these transactions, the user name and associated Secure Group Tags will be obtained from an Identity Services Engine server. If you are using ISE-PIC, the user name and associated ISE Secure Groups will be obtained. See Tasks for Integrating the ISE/ISE-PIC Service, on page 153.
- **Transparently identify users with ASA** – Users are identified by the current IP address-to-user name mapping received from a Cisco Adaptive Security Appliance (for remote users only). This option is available when AnyConnect Secure Mobility is enabled and integrated with an ASA. The user name will be obtained from the ASA, and associated directory groups will be obtained from the authentication realm or sequence specified on the Web Security Appliance . See Remote Users, on page 238.
- **Transparently identify users with authentication realms** – This option is available when one or more authentication realms are configured to support transparent identification using one of the following authentication servers:

- **Active Directory** – Create an NTLM or Kerberos authentication realm and enable transparent user identification. In addition, you must deploy a separate Active Directory agent such as Cisco's Context Directory Agent. For more information, see Transparent User Identification with Active Directory, on page 93.
- **LDAP** – Create an LDAP authentication realm configured as an eDirectory, and enable transparent user identification. For more information, see Transparent User Identification with LDAP, on page 94.

AsyncOS for Web communicates at regular intervals with eDirectory or an Active Directory agent to maintain mappings that match authenticated user names to their current IP addresses.

### Transparent User Identification with Active Directory

Active Directory does not record user log-in information in a format that is easily queried by other systems such as the Web Security Appliance . Active Directory agents, such as Cisco's Context Directory Agent (CDA), are necessary to query the Active Directory security event logs for information about authenticated users.



**Note** CDA is not supported by Active Directory in Windows Server 2016. You can use Identity Services Engine (ISE) or ISE Passive Identity Controller (ISE-PIC) service to receive user information and achieve transparent user identification. You must configure identification profiles and relevant access policies, and decryption policies that use CDA, with ISE/ISE-PIC information when you switch from CDA to ISE/ISE-PIC.

AsyncOS for Web communicates with the Active Directory agent to maintain a local copy of the IP-address-to-user-name mappings. When AsyncOS for Web needs to associate an IP address with a user name, it first checks its local copy of the mappings. If no match is found, it queries an Active Directory agent to find a match.

For more information on installing and configuring an Active Directory agent, see the section "Setting Up an Active Directory Agent to Provide Information to the Web Security Appliance " below.

Consider the following when you identify users transparently using Active Directory:

- Transparent user identification with Active Directory works with an NTLM or Kerberos authentication scheme only. You cannot use it with an LDAP authentication realm that corresponds to an Active Directory instance.
- Transparent user identification works with the versions of Active Directory supported by an Active Directory agent.
- You can install a second instance of an Active Directory agent on a different machine to achieve high availability. When you do this, each Active Directory agent maintains IP-address-to-user-name mappings independently of the other agent. AsyncOS for Web uses the backup Active Directory agent after three unsuccessful ping attempts to the primary agent.
- The Active Directory agent uses on-demand mode when it communicates with the Web Security Appliance .
- The Active Directory agent pushes user log-out information to the Web Security Appliance . Occasionally, some user log-out information is not recorded in the Active Directory security logs. This can happen if the client machine crashes, or if the user shuts down the machine without logging out. If there is no user log-out information in the security logs, an Active Directory agent cannot inform the appliance that the

IP address no longer is assigned to that user. To obviate this possibility, you can define how long AsyncOS caches the IP-address-to-user mappings when there are no updates from an Active Directory agent. For more information, see Using the CLI to Configure Advanced Transparent User Identification Settings, on page 96.

- The Active Directory agent records the `sAMAccountName` for each user logging in from a particular IP address to ensure the user name is unique.
- The client IP addresses that the client machines present to the Active Directory server and the Web Security Appliance must be the same.
- AsyncOS for Web searches only direct parent groups for a user. It does not search nested groups.

#### Setting Up an Active Directory Agent to Provide Information to the Web Security Appliance

Because AsyncOS for Web cannot obtain client IP addresses directly from Active Directory, it must obtain IP-address-to-user-name mapping information from an Active Directory agent.

Install an Active Directory agent on a machine in the network that is accessible to the Web Security Appliance , and which can communicate with all visible Windows domain controllers. For best performance, this agent should be physically as close as possible to the Web Security Appliance . In smaller network environments, you may want to install the Active Directory agent directly on the Active Directory server.

**Note** The Active Directory agent instance used to communicate with the Web Security Appliance can also support other appliances, including Cisco's Adaptive Security Appliance and other Web Security Appliance s.

#### Obtaining, Installing, and Configuring Cisco's Context Directory Agent

You can find information about downloading, installing, and configuring the Cisco Context Directory Agent here: http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda10.html.

**Note** The Web Security Appliance and Active Directory agent communicate with each other using the RADIUS protocol. The appliance and the agent must be configured with the same shared secret to obfuscate user passphrases. Other user attributes are not obfuscated.

### Transparent User Identification with LDAP

AsyncOS for Web can communicate with an eDirectory server configured as a Lightweight Directory Access Protocol (LDAP) realms maintaining IP-address-to-user-name mappings. When a user logs in through an eDirectory client, the user is authenticated against the eDirectory server. When authentication succeeds, the client IP address is recorded in the eDirectory server as an attribute ( NetworkAddress ) of the user who logged in.

Consider the following when you identify users transparently using LDAP (eDirectory):

- The eDirectory client must be installed on each client workstation, and end users must use it to authenticate against an eDirectory server.
- The LDAP tree used by the eDirectory client log-in must be the same LDAP tree configured in the authentication realm.

- If the eDirectory clients use multiple LDAP trees, create an authentication realm for each tree, and then create an authentication sequence that uses each LDAP authentication realm.
- When you configure the LDAP authentication realm as an eDirectory, you must specify a Bind DN for the query credentials.
- The eDirectory server must be configured to update the NetworkAddress attribute of the user object when a user logs in.
- AsyncOS for Web searches only direct parent groups for a user. It does not search nested groups.
- You can use the NetworkAddress attribute for an eDirectory user to determine the most-recent log-in IP address for the user.

## Rules and Guidelines for Transparent User Identification

Consider the following rules and guidelines when using transparent user identification with any authentication server:

- When using DHCP to assign IP addresses to client machines, ensure the IP-address-to-user-name mappings are updated on the Web Security Appliance more frequently than the DHCP lease. Use the `tuiconfig` CLI command to update the mapping update interval. For more information, see Using the CLI to Configure Advanced Transparent User Identification Settings, on page 96.
- If a user logs out of a machine and another user logs into the same machine before the IP-address-to user-name mapping is updated on the Web Security Appliance , then the Web Proxy logs the client as the previous user.
- You can configure how the Web Proxy handles transactions when transparent user identification fails. It can grant users guest access, or it can force an authentication prompt to appear to end users.
- When a user is shown an authentication prompt due to failed transparent user identification, and the user then fails authentication due to invalid credentials, you can choose whether to allow the user guest access.
- When the assigned Identification Profile uses an authentication sequence with multiple realms in which the user exists, AsyncOS for Web fetches the user groups from the realms in the order in which they appear in the sequence.
- When you configure an Identification Profile to transparently identify users, the authentication surrogate must be IP address. You cannot select a different surrogate type.
- When you view detailed transactions for users, the Web Tracking page shows which users were identified transparently.
- You can log which users were identified transparently in the access and WC3 logs using the `%m` and `x-auth-mechanism` custom fields. A log entry of `SSO_TUI` indicates that the user name was obtained by matching the client IP address to an authenticated user name using transparent user identification. (Similarly, a value of `SSO_ASA` indicates that the user is a remote user and the user name was obtained from a Cisco ASA using AnyConnect Secure Mobility.)

## Configuring Transparent User Identification

Configuring transparent user identification and authorization is detailed in Overview of Acquire End-User Credentials, on page 87 . The basic steps are:

- Create and order authentication realms.
- Create Identification Profiles to classify users and client software.

- Create policies to manage web requests from the identified users and user groups.

## Using the CLI to Configure Advanced Transparent User Identification Settings

AsyncOS for Web provides the following TUI-related CLI commands:

- **`tuiconfig`** – Configure advanced settings associated with transparent user identification. Batch mode can be used to configure multiple parameters simultaneously.
  - **`Configure mapping timeout for Active Directory agent`** – Length of time, in minutes, IP-address-to-user mappings are cached for IP addresses retrieved by the AD agent when there are no updates from the agent.
  - **`Configure proxy cache timeout for Active Directory agent`** – Length of time, in seconds, proxy-specific IP-address-to-user mappings are cached; valid values range from five to 1200 seconds. The default and recommended value is 120 seconds. Specifying a lower value may negatively affect proxy performance.
  - **`Configure mapping timeout for Novell eDirectory`** – Length of time, in seconds, IP-address to-user mappings are cached for IP addresses retrieved from the eDirectory server when there are no updates from the server.
  - **`Configure query wait time for Active Directory agent`** – The length of time, in seconds, to wait for a reply from the Active Directory agent. When the query takes more than this value, transparent user identification is considered to have failed. This limits the authentication delay experienced by the end user.
  - **`Configure query wait time for Novell eDirectory`** – The length of time, in seconds, to wait for a reply from the eDirectory server. When the query takes more than this value, transparent user identification is considered to have failed. This limits the authentication delay experienced by the end user.

The Active Directory settings apply to all AD realms using an AD agent for transparent user identification. The eDirectory settings apply to all LDAP realms using eDirectory for transparent user identification.

If validation fails for any one parameter, none of the values will be changed.

- **`tuistatus`** – This command provides the following AD-related subcommands:
  - **`adagentstatus`** – Displays the current status of all AD agents, as well as information about their connections with the Windows domain controllers.
  - **`listlocalmappings`** – Lists all IP-address-to-user-name mappings stored on the Web Security Appliance , as retrieved by the AD agent(s). It does not list entries stored on the agent(s), nor does it list mappings for which queries are currently in progress.

## Configuring Single-Sign-on

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

For Internet Explorer, be sure the Redirect Hostname is the short host name (containing no dots) or the NetBIOS name rather than a fully qualified domain. Alternatively, you can add the appliance host name to Internet Explorer's Local intranet zone (Tools > Internet options > Security tab); however, this will be required on

every client. For more information about this, see How do I properly set up NTLM with SSO (credentials sent transparently)?

With Firefox and other non-Microsoft browsers, the parameters **network.negotiate-auth.delegation-uris**, **network.negotiate-auth.trusted-uris** and **network.automatic-ntlm-auth.trusted-uris** must be set to the transparent-mode Redirect Hostname. You also can refer to Firefox is not sending authentication credentials transparently (SSO). This article provides general information about changing Firefox parameters.

For information about the Redirect Hostname, see Configuring Global Authentication Settings, on page 112, or the CLI command `sethostname`.

# Creating a Service Account in Windows Active Directory for Kerberos Authentication in High Availability Deployments

Use this procedure if you are having issues with high availability with Kerberos authentication. Scenarios, where issues may arise when using Kerberos Authentication in High Availability Deployments are:

- The servicePrincipalName of the high availability hostname is added to multiple machine accounts in the Active Directory.
- Kerberos authentication works if the servicePrincipalName has been added to single machine account in the Active Directory. When the primary node changes, high availability may be impacted, because different appliance nodes use different encryption strings to decrypt Kerberos service tickets.

### Before you begin

- Choose the user name to be used for high availability with Kerberos authentication. We recommend creating a new user name, which will be used solely for this purpose.
- If you prefer using an existing user name:
  - Set a password, if the user name does not have one.
  - In the user account properties dialog box (in Active Directory users and computers):

    Ensure that the User must change password at next logon check box is unchecked.

    Check the Password never expires check box.

### Procedure

**Step 1** Create a new user name in Active Directory users and computers.

- Specify a password.
- Uncheck the User must change password at next logon check box.
- Check the Password never expires check box.

**Step 2** Check if the SPN of the high availability hostname is associated with the Active Directory user object created or chosen. SPN consists of a http/ prefix, and is suffixed with the appliance's high availability hostname. Ensure that the clients are able to resolve the hostname.

**a.** Use the `setspn -q` command in Windows, to query for any existing association.

Example: `setspn -q http/highavail.com`

In this example, highavail.com is the appliance's high availability hostname.

**b.** Remove, or add the SPN depending on the results of the query:

**Note**
Kerberos HA service account passwords can only include letters, numbers, spaces and characters ~ ! @ # % ^ & () _ - {} ' / [] : ; , | + = * ? <>. If any of these 3 special characters $, `, or " are used in the Kerberos HA service account password, it will result in a failure during pre-authentication from both GUI and CLI. However, authentication is successful with all kinds of characters used in the password.

| Query Result | Action |
|---|---|
| No such SPN found. | Associate the SPN of the high availability hostname is associated with the Active Directory user object.<br>• Use the `setspn -s` command:<br>`setspn -s http/highavail.com hausername`<br>In this example, highavail.com is the appliance's high availability hostname, and hausername is the user name created or chosen. |
| Existing SPN found!<br>The common name (CN) shows the user name created or chosen.<br>Example: CN = hausername | No further action is necessary in the Active Directory. |
| Existing SPN found!<br>The common name (CN) does not show the user name created or chosen. | **a.** Remove the SPN.<br>Use the `setspn -d` command:<br>`setspn -d http/highavail.com johndoe`<br>In this example, highavail.com is the appliance's high availability hostname, and johndoe is the user name to be disassociated.<br>**b.** Add the SPN.<br>Use the `setspn -s` command:<br>`setspn -s http/highavail.com hausername`<br>In this example, highavail.com is the appliance's high availability hostname, and hausername is the user name created or chosen. |

**Note**
Ensure that keytab authentication is enabled in the relevant Active Directory realm. See Creating an Active Directory Realm for Kerberos Authentication Scheme, on page 100. For realms already created, edit the realm, and enable the keytab authentication.

# 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.

### Authentication Failover

In the current realm setup, there are one primary AD or LDAP and two backup servers. If the first primary server is not reachable, the query reaches to the first backup server. If the first backup server is also not reachable, the query reaches to the second server.

*Table 4: Failover time using IPFW rule*

| Failover time | Failover time taken from primary to secondary backup in seconds |
|---|---|
| To break the connection between primary AD and Web Security Appliance | 75 to 80 |
| To break the connection between primary AD andWeb Security Appliance and also to break connection between first backup and Web Security Appliance | 180 to 250 |
| Reboot primary AD | 42 secs |
| Power off Primary AD | 75 to 80 |
| Power off Primary AD and first backup server | 180 to 250 |

If more than one servers are down, Web Security Appliance retries to establish connection until a working domain controller is found.

- External Authentication, on page 100
- Creating an Active Directory Realm for Kerberos Authentication Scheme, on page 100
- How to Create an Active Directory Authentication Realm (NTLMSSP and Basic), on page 104
- Creating an LDAP Authentication Realm, on page 107
- About Deleting Authentication Realms, on page 112
- Configuring Global Authentication Settings, on page 112

### Related Topics

- Authentication Sequences, on page 117
- RADIUS User Authentication, on page 512

# External Authentication

You can authenticate users through an external LDAP or RADIUS server.

## Configuring External Authentication through an LDAP Server

### Before you begin

Create an LDAP authentication realm and configure it with one or more external authentication queries. Creating an LDAP Authentication Realm, on page 107.

### Procedure

**Step 1** Enable external authentication on the appliance:

a) Navigate to **System Administration** > **Users**.
b) Click **Enable** in the External Authentication section.
c) Configure the options:

| Option | Description |
|---|---|
| Enable External Authentication | — |
| Authentication Type | Select LDAP. |
| External Authentication Cache Timeout | The number of seconds AsyncOS stores the external authentication credentials before contacting the LDAP server again to re-authenticate. Default is zero (0). |
| LDAP External Authentication Query | A query configured with the LDAP realm. |
| Timeout to wait for valid response from server. | The number of seconds AsyncOS waits for a response to the query from the server. |
| Group Mapping | For each group name in the directory, assign a role. |

**Step 2** Submit and commit your changes.

## Enabling RADIUS External Authentication

See Enabling External Authentication Using RADIUS, on page 512.

# Creating an Active Directory Realm for Kerberos Authentication Scheme

### Before you begin

- Ensure that the appliance is configured in Standard mode (not Cloud Connector Mode).

- If you are setting up high availability, ensure that you also enable the **Use keytab authentication** check box in the Kerberos High Availability section, specified in **step 9**.

  If your appliance resides behind a HTTP/HTTPS traffic distribution device like a load balancer, you must associate the SPN of the traffic distribution device in the Active Directory with a user account, and enter the credentials of that user account in the Kerberos High Availability section. The SPN of the first device that redirects traffic in the network topology should be added. For example, if client devices' outbound network traffic passes through a traffic manager, a load balancer, and then to the Web Security Appliance , the SPN for the traffic manager should be added to a user account on the Active Directory, and the user credentials should be entered in this section. This is because the traffic manager is the first device that encounters client devices' traffic.

- Prepare the Active Directory Server.
  - Install Active Directory on one of these servers: Windows server 2003, 2008, 2008R2, 2012, 2016 (for coeus 11.8, 12.0, 12.5, 14.0, and 14.5), or 2019 (for coeus 14.5 only).

    You can install Active Directory Windows server 2019 for coeus 12.5.
  - Create a user on the Active Directory server:
    - Create a user on the Active Directory server that is a member of the Domain Admins or Account Operators group.

      Or
    - Create a user name with the following permissions:
      - Active Directory permissions Reset Password
      - Validated write to servicePrincipalName
      - Write account restrictions
      - Write dNShost name
      - Write servicePrincipalName

        These are the minimal Active Directory permissions required by a user name to join an appliance to the domain and ensure its complete functioning.
  - Join your client to the domain. Supported clients are Windows XP, Windows 10 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 that you have the rights and domain information needed to join the Web Security Appliance to the Active Directory domain you want 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 Appliance s have identical properties defined on each appliance.
- Web Security Appliance configuration:
  - In explicit mode, the Web Security Appliance host name (CLI command `sethostname`) and the proxy name configured in the browser must be the same.
  - In transparent mode, the Web Security Appliance host name must be the same as the Redirect Hostname (see Configuring Global Authentication Settings, on page 112). Further, the Web Security Appliance host name and Redirect Hostname must be configured prior to creating a Kerberos realm.
- Be aware that after you commit the new realm, you cannot change a protocol of realm authentication.
- Note that Single Sign On (SSO) must be configured on client browsers; see Configuring Single-Sign-on, on page 96.
- To simplify use of logs, customize the access log to use the %m custom field parameter. See Customizing Access Logs, on page 460.

**Note** Kerberos HA service account passwords can only include letters, numbers, spaces and characters ~ ! @ # % ^ & () _ - {} ' / [] : ; , | + = * ? <>. If any of these 3 special characters $, `, or " are used in the Kerberos HA service account password, it will result in a failure during pre-authentication from both GUI and CLI. However, authentication is successful with all kinds of characters used in the password.

## Procedure

**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.<br>**Tip**<br>If this option is not available use the `setntlmsecuritymode` 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.<br>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. |
| Enable Trusted Domain Lookup | **Enable Trusted Domain Lookup** option is added in the **Active Directory Account** section (**Network** > **Authentication** > **Add Realm**) to control the behavior of the trusted domain lookup for the realm.<br>The option is enabled by default. |

b) Click **Join Domain**.

**Note**
If you attempt to join a domain you have already joined (even if you use the same credentials), existing connections will be closed, as the Active Directory will send a new set of keys to all clients including this Web Security Appliance . Affected clients will need to log off and log back in again.

c) Provide login credentials (user name and passphrase) for the account on the Active Directory, and click Create Account.

**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 Context Directory agent is installed and the shared secret used to access it.<br>(Optional) Enter the server name for the machine where a backup Context 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. The selection of this option enables SMB signing to:<br>• Place the digital signature when the appliance connects to the Active Directory.<br>• Prevent man-in-the-middle attacks. |

**Step 9** If you will use high availability, check the **Use keytab authentication** check box in the Kerberos High Availability section.

a) Enter the Username and Password.

Enter the username of Active Directory user name associated with SPN(s) corresponding to the IP address or hostname of the high availability cluster. Do not include the domain name with the user name (for example, enter 'johndoe', rather than 'DOMAIN\johndoe', or 'johndoe@domain'). See Creating a Service Account in Windows Active Directory for Kerberos Authentication in High Availability Deployments, on page 97 for specific information about creating a service account that will be used for authentication in high availability deployments.

b) Repeat this step for all appliances in the high availability cluster.

**Note**
If your appliance resides behind a HTTP/HTTPS traffic distribution device like a load balancer, you should associate the SPN of the traffic distribution device in the Active Directory with a user account, and enter the credentials of that user account in the Kerberos High Availability section. The SPN of the first device that redirects traffic in the network topology should be added. For example, if client devices' outbound network traffic passes through a traffic manager, a load balancer, and then to the Web Security Appliance , the SPN for the traffic manager should be added to a user account on the Active Directory, and the user credentials should be entered in this section. This is because the traffic manager is the first device that encounters client devices' traffic.

**Step 10** (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 Using Multiple NTLM Realms and Domains, on page 112.

**Step 11** Troubleshoot any issues found during testing. See Troubleshooting Tools for Authentication Issues , on page 557.

**Step 12** Submit and commit your changes.

### What to do next

Create an Identification Profile that uses the Kerberos authentication scheme. Classifying Users and Client Software, on page 131.

# How to Create an Active Directory Authentication Realm (NTLMSSP and Basic)

## Prerequisites for Creating an Active Directory Authentication Realm (NTLMSSP and Basic)

- 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 topic 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 Appliance s have identical properties defined on each appliance.
- Be aware that once you commit the new realm, you cannot change a realm's authentication protocol.

- The Web Security Appliance needs to connect to the domain controllers for all trusted domains, and to the configured domain controllers into the NTLM realm. For authentication to work correctly, you need to open the following ports to all domain controllers on the internal domain and on the external domain:
  - LDAP (389 UDP and TCP)
  - Microsoft SMB (445 TCP)
  - Kerberos (88 TCP)
  - End-point resolution – port mapper (135 TCP) Net Log-on fixed port
- For NTLMSSP, single sign on (SSO) can be configured on client browsers. See Configuring Single-Sign-on, on page 96.

## About 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.

## Creating an Active Directory Authentication Realm (NTLMSSP and Basic)

### Before you begin

Ensure that the higher range ports in the appliance (49152-65535) are unblocked in your firewall. These ports are required to perform the asynchronous group lookup requests. Blocking these ports may cause intermittent authentication failure.

### Procedure

**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:

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. |
| NetBIOS domain name | If the network uses NetBIOS, provide the domain name. |
| 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.<br>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. |
| Enable Trusted Domain Lookup | **Enable Trusted Domain Lookup** option is added in the **Active Directory Account** section (**Network** > **Authentication** > **Add Realm**) to control the behavior of the trusted domain lookup for the realm.<br>The option is enabled by default. |

b) Click **Join Domain**.

**Note**
If you attempt to join a domain you have already joined (even if you use the same credentials), existing connections will be closed, as the Active Directory will send a new set of keys to all clients including this Web Security Appliance . Affected clients will need to log off and log back in again.

c) Enter the sAMAccountName user name and passphrase 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 Context Directory agent is installed and the shared secret used to access it.<br>(Optional) Enter the server name for the machine where a backup Context 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. The selection of this option enables SMB signing to:<br>• Place the digital signature when the appliance connects to the Active Directory.<br>• Prevent man-in-the-middle attacks. |

**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 Appliance s have identical properties defined on each appliance.

### Procedure

**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 | Choose the version of LDAP, and choose whether or not to use Secure LDAP.<br>The appliance supports LDAP versions 2 and 3. Secure LDAP requires LDAP version 3.<br>Choose whether or not this LDAP server supports Novell eDirectory to use with transparent user identification. |

| Setting | Description |
|---|---|
| LDAP Server | Enter the LDAP server IP address or hostname and its port number. You can specify up to three servers.<br><br>The hostname must be a fully-qualified domain name. For example, `ldap.example.com`. An IP address is required only if the DNS servers configured on the appliance cannot resolve the LDAP server hostname.<br><br>The default port number for Standard LDAP is 389. The default number for Secure LDAP is 636.<br><br>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.<br><br>**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.<br><br>From AsyncOS version 11.5 onwards, you can specify the source interface for LDAP/NTLM (Domain Controller communication). Select the **Set Source Interface** check box, and then select the Source Interface from the drop-down. |
| LDAP Persistent Connections<br><br>(under the Advanced section) | Choose one of the following values:<br><br>• **Use persistent connections (unlimited)**. Use existing connections. If no connections are available a new connection is opened.<br><br>• **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.<br><br>• **Do not use persistent connections.** Always create a new connection to the LDAP server. |

| Setting | Description |
|---|---|
| User Authentication | Enter values for the following fields:<br>**Base Distinguished Name (Base DN)**<br>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 `object-value`. For example `dc=companyname, dc=com`.<br>**Note**<br>After you upgrade to this release, you cannot perform the Start Test for LDAP authentication if this field is empty.<br>**User Name Attribute**<br>Choose one of the following values:<br>• **uid**, **cn**, and **sAMAccountName.** Unique identifiers in the LDAP directory that specify a username.<br>• **custom.** A custom identifier such as `UserAccount`.<br>**User Filter Query**<br>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.<br>Choose one of the following values:<br>• **none.** Filters any user.<br>• **custom.** Filters a particular group of users. |
| Query Credentials | Choose whether or not the authentication server accepts anonymous queries.<br>If the authentication server does accept anonymous queries, choose **Server Accepts Anonymous Queries**.<br>If the authentication server does not accept anonymous queries, choose **Use Bind DN** and then enter the following information:<br>• **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.<br>• **Passphrase.** The passphrase associated with the user you enter in the Bind DN field.<br>The following text lists some example users for the Bind DN field:<br>cn=administrator,cn=Users,dc=domain,dc=com<br>sAMAccountName=jdoe,cn=Users,dc=domain,dc=com.<br>If the LDAP server is an Active Directory server, you may also enter the Bind DN username as "DOMAIN\username." |

**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 | Choose the LDAP attribute which lists all users that belong to this group.<br>Choose one of the following values:<br>• **member** and **uniquemember.** Unique identifiers in the LDAP directory that specify group members.<br>• **custom.** A custom identifier such as `UserInGroup`. |
| Attribute that Contains the Group Name | Choose the LDAP attribute which specifies the group name that can be used in the policy group configuration.<br>Choose one of the following values:<br>• **cn.** A unique identifier in the LDAP directory that specifies the name of a group.<br>• **custom.** A custom identifier such as `FinanceGroup`. |
| Query String to Determine if Object is a Group | Choose an LDAP search filter that determines if an LDAP object represents a user group.<br>Choose one of the following values:<br>• **objectclass=groupofnames**<br>• **objectclass=groupofuniquenames**<br>• **objectclass=group**<br>• **custom.** A custom filter such as `objectclass=person`.<br>**Note:** The query defines the set of authentication groups which can be used in policy groups. |

| User Object Setting | Description |
|---|---|
| Group Membership Attribute Within User Object | Choose the attribute which list all the groups that this user belongs to.<br>Choose one of the following values:<br>• **memberOf.** Unique identifiers in the LDAP directory that specify user members.<br>• **custom.** A custom identifier such as `UserInGroup`. |
| Group Membership Attribute is a DN | Specify whether the group membership attribute is a distinguished name (DN) which refers to an LDAP object. For Active Directory servers, enable this option.<br>When this is enabled, you must configure the subsequent settings. |
| Attribute that Contains the Group Name | When the group membership attribute is a DN, this specifies the attribute that can be used as group name in policy group configurations.<br>Choose one of the following values:<br>• **cn.** A unique identifier in the LDAP directory that specifies the name of a group.<br>• **custom.** A custom identifier such as `FinanceGroup`. |

| User Object Setting | Description |
|---|---|
| Query String to Determine if Object is a Group | Choose an LDAP search filter that determines if an LDAP object represents a user group.<br>Choose one of the following values:<br>• **objectclass=groupofnames**<br>• **objectclass=groupofuniquenames**<br>• **objectclass=group**<br>• **custom.** A custom filter such as `objectclass=person`.<br>**Note:** The query defines the set of authentication groups which can be used in Web Security Manager policies. |

**Step 7** (Optional) Configure external LDAP authentication for users.

a) Select **External Authentication Queries**.

b) Identify the user accounts:.

| Base DN | The Base DN to navigate to the correct location in the LDAP directory tree to begin a search. |
|---|---|
| Query String | The query to return the set of authentication groups, for example:<br>`(&(objectClass=posixAccount)(uid={u}))`<br>or<br>`(&(objectClass=user)(sAMAccountName={u}))` |
| Attribute containing the user's full name | The LDAP attribute, for example, displayName or gecos . |

c) (Optional) Deny login to expired accounts based on RFC 2307 account expiration LDAP attributes.

d) Provide a query to retrieve group information for users.

If a user belongs to multiple LDAP groups with different user roles, AsyncOS grants the user the permissions for the most restrictive role.

| Base DN | The Base DN to navigate to the correct location in the LDAP directory tree to begin a search. |
|---|---|
| Query String | `(&(objectClass=posixAccount)(uid={u}))` |
| Attribute containing the user's full name | `gecos` |

**Step 8** (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 Using Multiple NTLM Realms and Domains, on page 112.

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

**Step 9** Submit and commit your changes.

### What to do next

Create an Identification Profile that uses the Kerberos authentication scheme. See Classifying Users and Client Software, on page 131.

### Related Topics

- External Authentication, on page 100

## 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, on page 119
- Failed Authorization: Allowing Re-Authentication with Different Credentials, on page 124

## Procedure

**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:<br>• **Permit traffic to proceed without authentication.** Processing continues as if the user was authenticated.<br>• **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 Identification Profile policy, this setting determines how the Web Proxy identifies and logs the user as a guest in the access logs.<br>For more information on granting users guest access, see Granting Guest Access After Failed Authentication, on page 122. |
| Re-authentication<br>(Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction) | 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.<br>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.<br>**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.<br>For more information, see Failed Authorization: Allowing Re-Authentication with Different Credentials, on page 124. |
| Basic Authentication Token TTL | 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 passphrase and the directory groups associated with the user.<br>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. |

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 | This setting specifies whether or not the client sends the login credentials to the Web Proxy through an encrypted HTTPS connection.<br><br>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.<br><br>For more information, see Failed Authentication, on page 119. |
| HTTPS Redirect Port | Specify a TCP port to use for redirecting requests for authenticating users over an HTTPS connection.<br><br>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. |
| Redirect Hostname | Enter the short hostname of the network interface on which the Web Proxy listens for incoming connections.<br><br>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.<br><br>You can enter either the following values:<br><br>• **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. Be sure to enter the single word hostname that is DNS resolvable by the client and the Web Security Appliance . For example, if your clients are in domain mycompany.com and the interface on which the Web Proxy is listening has a full hostname of **`proxy.mycompany.com`** , then you should enter **`proxy`** in this field. Clients perform a lookup on proxy and they should be able to resolve **`proxy.mycompany.com`** .<br><br>• **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. The default value is the FQDN of the M1 or P1 interface, depending on which interface is used for proxy traffic. |
| Credential Cache Options:<br><br>Surrogate Timeout | 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).<br><br>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. |

| Setting | Description |
|---|---|
| Credential Cache Options:<br>Client IP Idle Timeout | 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.<br>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.<br>You might want to use this setting to reduce the vulnerability of users who leave their computers. |
| User Session Restrictions | This setting specifies whether or not authenticated users are allowed to access the Internet from multiple IP addresses simultaneously.<br>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.<br>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.<br>You can remove a specific user or all users from the authentication cache using the `authcache` CLI command. |
| Advanced | 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. |

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

| Setting | Description |
|---|---|
| Credential Encryption | 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.<br>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.<br>For more information, see Failed Authentication, on page 119. |

| Setting | Description |
|---|---|
| HTTPS Redirect Port | Specify a TCP port to use for redirecting requests for authenticating users over an HTTPS connection.<br>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. |
| Redirect Hostname | Enter the short host name of the network interface on which the Web Proxy listens for incoming connections.<br>When you enable Authentication Mode above, the Web Proxy uses this hostname in the redirection URL sent to clients for authenticating users.<br>You can enter either the following values:<br>• **Single word hostname.** You can enter the single word host name 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. Be sure to enter the single word host name that is DNS resolvable by the client and the Web Security Appliance . For example, if your clients are in domain mycompany.com and the interface on which the Web Proxy is listening has a full host name of `proxy.mycompany.com` , then you should enter `proxy` in this field. Clients perform a lookup on proxy and they should be able to resolve `proxy.mycompany.com` .<br>• **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. The default value is the FQDN of the M1 or P1 interface, depending on which interface is used for proxy traffic. |
| Credential Cache Options:<br>Surrogate Timeout | 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).<br>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. |
| Credential Cache Options:<br>Client IP Idle Timeout | 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.<br>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.<br>You might want to use this setting to reduce the vulnerability of users who leave their computers. |

| Setting | Description |
|---|---|
| User Session Restrictions | This setting specifies whether or not authenticated users are allowed to access the Internet from multiple IP addresses simultaneously.<br><br>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.<br><br>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.<br><br>You can remove a specific user or all users from the authentication cache using the `authcache` CLI command. |
| Advanced | 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.<br><br>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. |

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

# Authentication Sequences


- About Authentication Sequences, on page 117
- Creating Authentication Sequences, on page 118
- Editing And Reordering Authentication Sequences, on page 119
- Deleting Authentication Sequences, on page 119


## 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, on page 99.

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, configure a single Identification Profile for two authentication Realms ensuring that one identity is used for All Realms. The Realms must have mutual trust between them.

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, on page 99).
- If the Web Security Appliance is managed by a Security Management appliance, ensure that same-named authentication realms on different Web Security Appliance s 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.

### Procedure

**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

### Procedure

**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.

### Procedure

**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, on page 120
- Bypassing Authentication with Problematic User Agents , on page 120
- Bypassing Authentication, on page 121
- Permitting Unauthenticated Traffic While Authentication Service is Unavailable, on page 122

- Granting Guest Access After Failed Authentication, on page 122
- Failed Authorization: Allowing Re-Authentication with Different Credentials, on page 124


# About Failed Authentication

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

- **Client/user agent limitations.** Some client applications may not properly support authentication. You can bypass authentication for these clients by configuring Identification Profiles 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 with Problematic User Agents , on page 120
- Bypassing Authentication, on page 121
- Permitting Unauthenticated Traffic While Authentication Service is Unavailable, on page 122
- Granting Guest Access After Failed Authentication, on page 122


# Bypassing Authentication with Problematic User Agents

Some user agents are known to have authentication issues that can impact normal operations.

You should bypass authentication via the following user agents:

- Windows-Update-Agent
- MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT
- Microsoft BITS
- SLSSoapClient
- Akamai NetSession Interface
- Microsoft-CryptoAPI
- NCSI
- MSDW
- Gnotify
- msde
- Google Update



**Note** The access policies will still filter (based on URL categories) and scan (McAfee, Webroot) traffic as per the access policy setup.

### Procedure

**Step 1** Configure the Identification Profile to bypass authentication with the specified user agents:

a) Select **Web Security Manager** > **Identification Profile**.
b) Click **Add Identification Profile**.
c) Enter information:

| Option | Value |
|---|---|
| Name | User Agent AuthExempt Identification Profile |
| Insert Above | Set to the first profile in the processing order |
| Define Members by Subnet | Leave blank. |
| Define Members by Authentication | No Authentication Required. |

d) Click **Advanced** > **User Agents**.
e) Click **None Selected**.
f) Under Custom user Agents, specify the problematic User Agent strings.

**Step 2** Configure the Access Policy:

a) Choose **Web Security Manager** > **Access Policies**.
b) Click **Add Policy**.
c) Enter information:

| Option | Value |
|---|---|
| Policy Name | Auth Exemption for User Agents |
| Insert Above Policy | Set to the first policy in the processing order. |
| Identification Profile Policy | User Agent AuthExempt Identification Profile |
| Advanced | None |

**Step 3** Submit and commit your changes.

# Bypassing Authentication

| | Step | More Information |
|---|---|---|
| 1 | Create a custom URL category that contains the affected websites by configuring the Advanced properties. | Creating and Editing Custom URL Categories, on page 183 |

| | Step | More Information |
|---|---|---|
| 2 | Create an Identification Profile with these characteristics:<br>• Placed above all identities that require authentication.<br>• Includes the custom URL category.<br>• Includes affected client applications.<br>• Does not require authentication | Classifying Users and Client Software, on page 131 |
| 3 | Create a policy for the Identification Profile. | Creating a Policy , on page 219 |

### Related Topics

- Bypassing the Web Proxy

# PermittingUnauthenticatedTrafficWhileAuthenticationServiceisUnavailable

**Note** This configuration applies only when an authentication service is unavailable. It will not bypass authentication permanently. For alternative options, see About Failed Authentication, on page 120

### Procedure

**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 Identification Profile that Supports Guest Access, on page 123
2. Use an Identification Profile that Supports Guest Access in a Policy, on page 123
3. (Optional) Configure How Guest User Details are Logged, on page 123



**Note** If an Identification Profile allows guest access and there is no user-defined policy that uses that Identification Profile, users who fail authentication match the global policy of the applicable policy type. For example, if MyIdentificationProfile allows guest access and there is no user-defined Access Policy that uses MyIdentificationProfile, 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 Identification Profile that Supports Guest Access

### Procedure

**Step 1** Choose **Web Security Manager** > **Identification Profiles**.

**Step 2** Click **Add Identification Profile** 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 Identification Profile that Supports Guest Access in a Policy

### Procedure

**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 Identification Profiles** from the Identification Profiles And Users drop-down list (if not already chosen).

**Step 4** Choose a **profile** that supports guest access from the drop-down list in the Identification Profile column.

**Step 5** Click the **Guests (Users Failing Authentication)** radio button.

**Note**
If this option is not available it means the **profile** you chose is not configured to support guest access. Return to step 4 and choose another, or see Define an Identification Profile that Supports Guest Access, on page 123 to define a new one.

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

## Configure How Guest User Details are Logged

### Procedure

**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, on page 124
- Allowing Re-Authentication with Different Credentials, on page 124


## 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

### Procedure

**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.

## Supported Authentication Surrogates for Explicit Requests

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

## Supported Authentication Surrogates for Transparent Requests

**Note** See also the description of the Authentication Surrogates options in Classifying Users and Client Software, on page 131.

| Surrogate Types | Credential Encryption Disabled | | | Credential Encryption Enabled | | |
|---|---|---|---|---|---|---|
| Protocol: | HTTP | HTTPS | Native FTP | HTTP | HTTPS | Native FTP |
| 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.

### Related Topics

- Identification Profiles and Authentication , on page 137

## 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

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.

- Tracking Credentials for Reuse During a Session, on page 126
- Authentication and Authorization Failures, on page 127
- Credential Format, on page 127
- Credential Encryption for Basic Authentication, on page 127

## 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.

For Internet Explorer, be sure the Redirect Hostname is the short host name (containing no dots) or the NetBIOS name rather than a fully qualified domain. Alternatively, you can add the appliance host name to Internet Explorer's Local intranet zone (Tools > Internet options > Security tab); however, this will be required on

every client. For more information about this, see How do I properly set up NTLM with SSO (credentials sent transparently)?

With Firefox and other non-Microsoft browsers, the parameters **network.negotiate-auth.delegation-uris**, **network.negotiate-auth.trusted-uris** and **network.automatic-ntlm-auth.trusted-uris** must be set to the transparent-mode Redirect Hostname. You also can refer to Firefox is not sending authentication credentials transparently (SSO) . This article provides general information about changing Firefox parameters.

For information about the Redirect Hostname, see Configuring Global Authentication Settings, on page 112, or the CLI command `sethostname`.

# 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, on page 122
- Allowing Re-Authentication with Different Credentials, on page 124

# Credential Format

| Authentication Scheme | Credential Format |
|---|---|
| NTLMSSP | **`MyDomain\jsmith`** |
| Basic | **`jsmith`**<br>**`MyDomain\jsmith`**<br>**Note**<br>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.

### Procedure

**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.

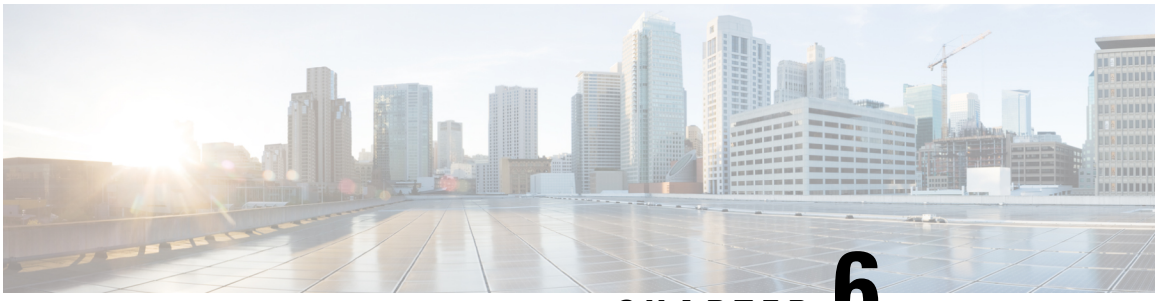
### What to do next

**Related Topics**

- Certificate Management, on page 533.

# Troubleshooting Authentication


- LDAP User Fails Authentication due to NTLMSSP, on page 557
- LDAP Authentication Fails due to LDAP Referral, on page 557
- Basic Authentication Fails, on page 558
- Users Erroneously Prompted for Credentials, on page 558
- HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 572
- Cannot Access URLs that Do Not Support Authentication, on page 578
- Client Requests Fail Upstream Proxy, on page 579



CHAPTER 6

# Classify End-Users for Policy Application

This topic contains the following sections:


- Overview of Classify Users and Client Software, on page 129
- Classify Users and Client Software: Best Practices, on page 130
- Identification Profile Criteria, on page 130
- Classifying Users and Client Software, on page 131
- Identification Profiles and Authentication , on page 137
- Troubleshooting Identification Profiles, on page 138
- Troubleshooting Surrogate Types in Identification Profiles, on page 139


## Overview of Classify Users and Client Software

Identification Profiles let you classify users and user agents (client software) for these purposes:

- Group transaction requests for the application of policies (except SaaS)
- Specification of identification and authentication requirements

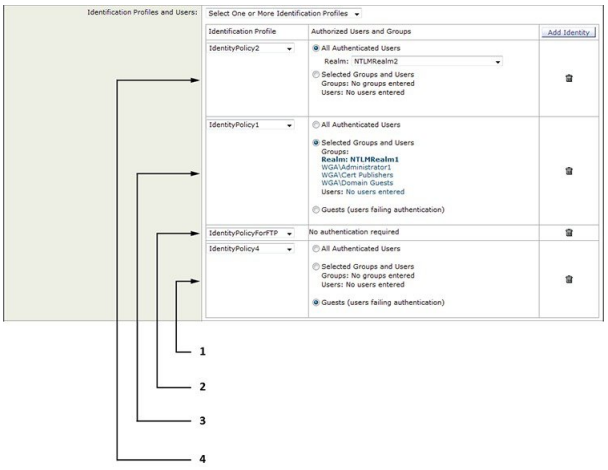
AsyncOS assigns an Identification Profile to every transaction:

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

AsyncOS processes Identification Profiles sequentially, beginning with the first. The global profile is the last profile.

An Identification Profile may include only one criterion. Alternately, Identification Profiles that include multiple criteria require that all the criteria are met.

One policy may call on multiple Identification Profiles:




| | |
|---|---|
| **1** | This Identification Profile allows guest access and applies to users who fail authentication. |
| **2** | Authentication is not used for this Identification Profile. |
| **3** | The specified user groups in this Identification Profile are authorized for this policy. |
| **4** | This Identification Profile uses an authentication sequence and this policy applies to one realm in the sequence. |

# Classify Users and Client Software: Best Practices

- Create fewer, more general Identification Profiles that apply to all users or fewer, larger groups of users. Use policies, rather than profiles, for more granular management.
- Create Identification Profiles with unique criteria.
- If deployed in transparent mode, create an Identification Profile for sites that do not support authentication. See Bypassing Authentication, on page 121.

# Identification Profile Criteria

These transaction characteristics are available to define an Identification Profile:

| Option | Description |
|---|---|
| Subnet | The client subnet must match the list of subnets in a policy. |
| Protocol | The protocol used in the transaction: HTTP, HTTPS, SOCKS, or native FTP. |
| Port | The proxy port of the request must be in the Identification Profile's list of ports, if any are 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 application) making the request must be in the Identification Profile's list of user agents, if any are listed. Some user agents cannot handle authentication, therefore creating an profile that does not require authentication is necessary. User agents include programs such as updaters and browsers, such as Internet Explorer and Mozilla Firefox. |
| URL Category | The URL category of the request URL must be in the Identification Profile's list of URL categories, if any are listed. |
| Authentication requirements | If the Identification Profile requires authentication, the client authentication credentials must match the Identification Profile's authentication requirements. |

# Classifying Users and Client Software

### Before you begin

- Create authentication realms. See How to Create an Active Directory Authentication Realm (NTLMSSP and Basic), on page 104 or Creating an LDAP Authentication Realm, on page 107 .
- Be aware that when you commit changes to Identification Profiles, end-users must re-authenticate.
- If you are in Cloud Connector mode, be aware that an additional Identification Profile option is available: Machine ID. See Identifying Machines for Policy Application, on page 62.
- (Optional) Create authentication sequences. See Creating Authentication Sequences, on page 118
- (Optional) Enable Secure Mobility if the Identification Profile will include mobile users.
- (Optional) Understand authentication surrogates. See Tracking Identified Users, on page 125 .

### Procedure

**Step 1** Choose **Web Security Manager** > **Identification Profiles**.

**Step 2** Click **Add Profile** to add a profile.

**Step 3** Use the **Enable Identification Profile** check box to enable this profile, or to quickly disable it without deleting it.

**Step 4** Assign a unique profile **Name**.

**Step 5** A **Description** is optional.

**Step 6** From the **Insert Above** drop-down list, choose where this profile is to appear in the table.

**Note**
Position Identification Profiles that do not require authentication above the first Identification Profile that requires authentication.

**Step 7** In the **User Identification Method** section, choose an identification method and then supply related parameters; displayed options vary according to the method chosen.

a) Choose an identification method from the **User Identification Method** drop-down list.

| Option | Description |
|---|---|
| **Exempt from authentication/ identification** | Users are identified primarily by IP address. No additional parameters are required. |
| **Authenticate users** | Users are identified by the authentication credentials they enter. |
| **Transparently identify users with ISE** | Available when the ISE service is enabled (Network > Identity Services Engine). For these transactions, the user name and associated Secure Group Tags will be obtained from the Identity Services Engine. In ISE-PIC deployments, ISE groups and users information is received. For more information, see Tasks for Integrating the ISE/ISE-PIC Service, on page 153. |
| **Transparently identify users with authentication realm** | This option is available when one or more authentication realms are configured to support transparent identification. |

**Note**
When at least one Identification Profile with authentication or transparent identification is configured, the policy tables will support defining policy membership using user names, directory groups, and Secure Group Tags.

**Note**
Context Directory Agent (CDA) has reached End of Support. It is recommended configuring ISE/ISE-PIC for transparent user authentication instead of CDA.

b) Supply parameters appropriate to the chosen method. Not all of the sections described in this table are visible for each choice.

| | |
|---|---|
| Fallback to Authentication Realm or Guest Privileges | If user authentication is not available from ISE:<br>• **Support Guest Privileges** – The transaction will be allowed to continue, and will match subsequent policies for Guest users from all Identification Profiles.<br>• **Block Transactions** – Do not allow Internet access to users who cannot be identified by ISE.<br>• **Support Guest privileges** – Check this box to grant guest access to users who fail authentication due to invalid credentials. |

| | |
|---|---|
| Authentication Realm | **Select a Realm or Sequence**—Choose a defined authentication realm or sequence.<br>**Select a Scheme**—Choose an authentication scheme:<br>• **Kerberos**—The client is transparently authenticated by means of Kerberos tickets.<br>• **Basic** – The client always prompts users for credentials. After the user enters credentials, browsers typically offer a check box to remember the provided credentials. Each time the user opens the browser, the client either prompts for credentials or resends the previously saved credentials.<br>Credentials are sent unsecured as clear text (Base64). A packet capture between the client and Web Security Appliance can reveal the user name and passphrase.<br>• **NTLMSSP**—The client transparently authenticates using its Windows login credentials. The user is not prompted for credentials.<br>However, the client prompts the user for credentials under the following circumstances:<br>• The Windows credentials failed.<br>• The client does not trust the Web Security Appliance because of browser security settings.<br>Credentials are sent securely using a three-way handshake (digest style authentication). The passphrase is never sent across the connection.<br>• **Support Guest privileges** – Check this box to grant guest access to users who fail authentication due to invalid credentials. |
| Realm for Group Authentication | • **Select a Realm or Sequence** – Choose a defined authentication realm or sequence. |

| | |
|---|---|
| Authentication Surrogates | Specify how transactions will be associated with a user after successful authentication (options vary depending on Web Proxy deployment mode):<br>• **IP Address** – The Web Proxy tracks an authenticated user at a particular IP address. For transparent user identification, select this option.<br>• **Persistent Cookie** – 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.<br>• **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.<br>• **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.<br>• **Apply same surrogate settings to explicit forward requests** – Check to apply the surrogate used for transparent requests to explicit requests; enables credential encryption automatically. This option appears only when the Web Proxy is deployed in transparent mode.<br>**Note**<br>• You can define a timeout valve for the authentication surrogate for all requests in Global Authentication Settings.<br>• If you have configured the Identification Profiles to use different authentication surrogates (IP address, persistent cookie, session cookie, and so on), then the access is authenticated using the IP address surrogate even though the access matches Identification Profiles with other surrogates. |

**Step 8** In the **Membership Definition** section, supply membership parameters appropriate to the chosen identification method. Note that all of the options described in this table are not available to every User Identification Method.

| **Membership Definition** | |
|---|---|
| **Define Members by User Location** | Configure this Identification Profile to apply to: **Local Users Only**, **Remote Users Only**, or **Both**. This selection affects the available authentication settings for this Identification Profile. |
| **Define Members by Subnet** | Enter the addresses to which this Identification Profile should apply. You can use IP addresses, CIDR blocks, and subnets.<br>**Note**<br>If nothing is entered, the Identification Profile applies to all IP addresses. |

| | |
|---|---|
| **Define Members by Protocol** | Select the protocols to which this Identification Profile should apply; select all that apply:<br>• **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.<br>• **Native FTP** – Applies to native FTP requests only.<br>• **SOCKS** – Applies to SOCKS Policies only |
| **Define Members by Machine ID** | • **Do Not Use Machine ID in This Policy** – The user is not identified by machine ID.<br>• **Define User Authentication Policy Based on Machine ID** – The user is identified primarily by machine ID.<br>Click the Machine Groups area to display the Authorized Machine Groups page.<br>For each group you want to add, in the Directory Search field, start typing the name of the group to add and then click Add. You can select a group and click Remove to remove it from the list.<br>Click Done to return to the previous page.<br>Click the Machine IDs area to display the Authorized Machines page.<br>In the Authorized Machines, field, enter the machine IDs to associate with the policy then click Done.<br>**Note**<br>Authentication using Machine ID is supported only in Connector mode and requires Active Directory. |

| | |
|---|---|
| **Advanced** | Expand this section to define additional membership requirements.<br>• **Proxy Ports** – Specify one or more proxy ports used to access the Web Proxy. Enter port numbers separated by commas. For explicit forward connections, the proxy port is configured in the browser.<br>For transparent connections, this is the same as the destination port.<br>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.<br>• **URL Categories** – Select 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.<br>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.<br>• **User Agents** – Defines policy group membership by the user agents found in the client request. You can select some commonly defined agents, or define your own using regular expressions.<br>Also specify whether these user-agent specifications are inclusive or exclusive. In other words, whether membership definition includes only the selected user agents, or specifically excludes the selected user agents |

**Step 9** Submit and Commit Changes.

### What to do next

- Overview of Acquire End-User Credentials, on page 87
- Managing Web Requests Through Policies Task Overview, on page 215

# Enable/Disable an Identity

### Before you begin

- Be aware that disabling an Identification Profile removes it from associated policies.
- Be aware that re-enabling an Identification Profile does not re-associate it with any policies.

### Procedure

**Step 1** Choose **Web Security Manager** > **Identification Profiles**.

**Step 2** Click a profile in the Identification Profiles table to open the Identification Profile page for that profile.

**Step 3** Check or clear **Enable Identification Profile** immediately under Client/User Identification Profile Settings.

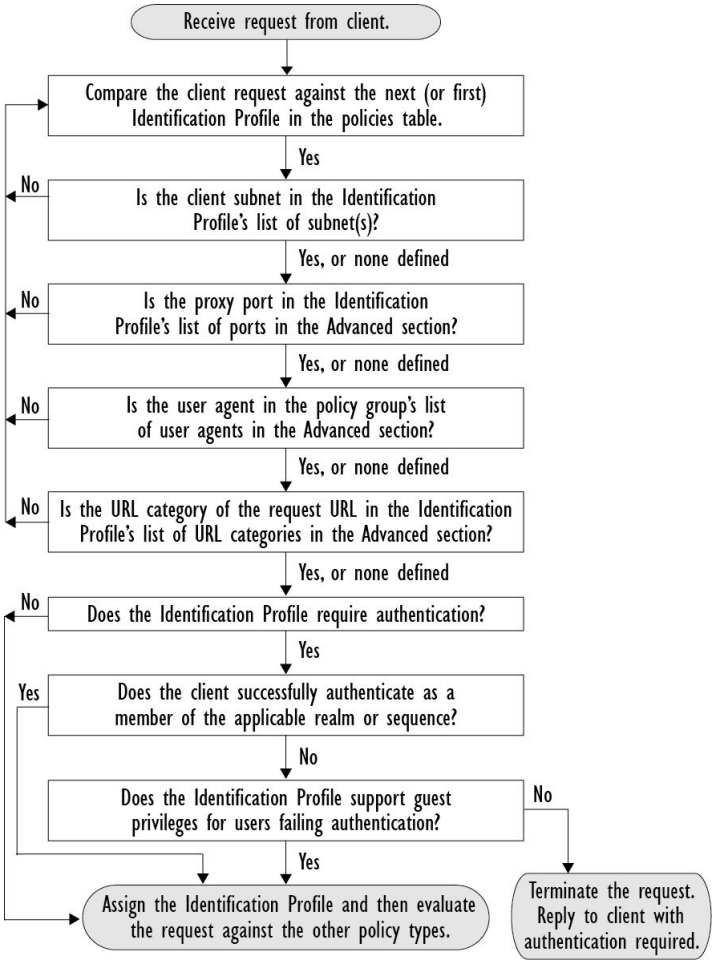
**Step 4** Submit and Commit Changes.

# Identification Profiles and Authentication

The following diagram shows how the Web Proxy evaluates a client request against an Identification Profile when the Identification Profiles is configured to use:

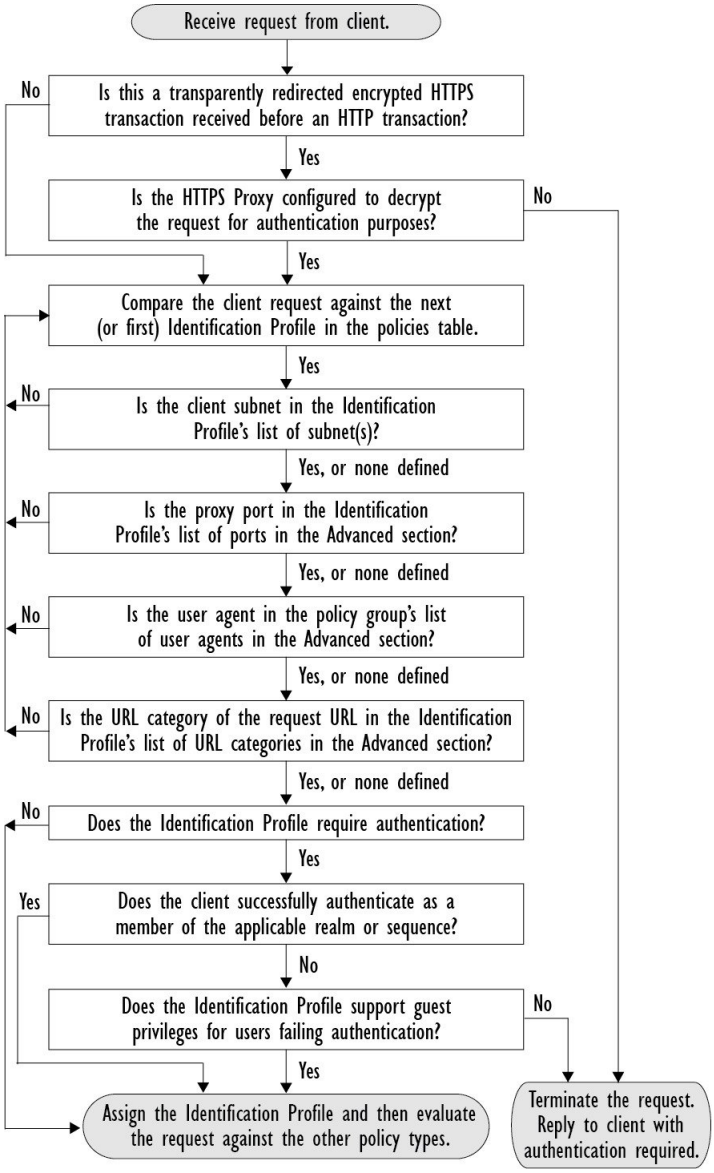
- No authentication surrogates
- IP addresses as authentication surrogates
- Cookies as authentication surrogates with transparent requests
- Cookies as authentication surrogates with explicit requests and credential encryption is enabled

***Figure 1: Identification Profiles and Authentication Processing – No Surrogates and IP-based Surrogates***




The following diagram shows how the Web Proxy evaluates a client request against an Identification Profile when the Identification Profile is configured to use cookies as the authentication surrogates, credential encryption is enabled, and the request is explicitly forwarded.

*Figure 2: Identification Profiles and Authentication Processing – Cookie-based Surrogates*



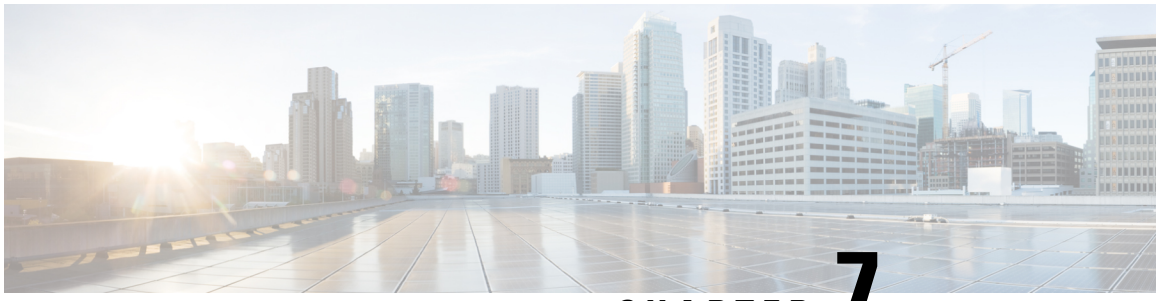

# Troubleshooting Identification Profiles


- Basic Authentication Problems, on page 558
- Policy Problems, on page 571
- Policy is Never Applied, on page 572
- Policy Troubleshooting Tool: Policy Trace, on page 573
- Upstream Proxy Problems, on page 579

# Troubleshooting Surrogate Types in Identification Profiles

When the Web Security Appliance is configured to use both IP address and cookie-based authentication surrogates and the access from the end-user matches both Identities, then the IP address overrides cookie-based authentication surrogates.

In a network with both shared and individual computers, it is recommended to create two different identification profiles based on IP addresses and subnets, which will determine whether IP or Cookie authentication surrogates are used.



CHAPTER 7

# SaaS Access Control

This topic contains the following sections:


- Overview of SaaS Access Control, on page 141
- Configuring the Appliance as an Identity Provider, on page 142
- Using SaaS Access Control and Multiple Appliances, on page 144
- Creating SaaS Application Authentication Policies, on page 144
- Configuring End-user Access to the Single Sign-on URL, on page 146


# 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 pass phrase.

SaaS Access Control only works with SaaS applications that require an authentication mechanism that is 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:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Configure the Web Security Appliance as an identity provider. | Configuring the Appliance as an Identity Provider, on page 142 |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | Create an authentication policy for the SaaS application. | Creating SaaS Application Authentication Policies, on page 144 |
| **Step 3** | Configure the SaaS application for single sign-on. | Configuring End-user Access to the Single Sign-on URL, on page 146 |
| **Step 4** | (Optional) Configue multiple Web Security Appliance s. | Using SaaS Access Control and Multiple Appliances, on page 144 |

# 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.

### Procedure

**Step 1** Choose **Network > Identity Provider for SaaS**.

**Step 2** Click **Edit Settings**.

**Step 3** Check **Enable SaaS Single Sign-on Service**.

**Step 4** Enter a virtual domain name in the **Identity Provider Domain Name** field.

**Step 5** Enter a unique text identifier in the **Identity Provider Entity ID** field (a URI formatted string is recommended).

**Step 6** Either upload or generate a certificate and key:

| Method | Additional Steps |
|---|---|
| **Upload a certificate and key** | **a.** Select **Use Uploaded Certificate and Key**.<br>**b.** In the **Certificate** field, click Browse; locate the file to upload.<br>**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.<br>**c.** In the **Key** field, click Browse; locate the file to upload.<br>If the key is encrypted, select **Key is Encrypted**.<br>**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.<br>**d.** Click **Upload Files**.<br>**e.** Click **Download Certificate** to download a copy of the certificate for transfer to the SaaS applications with which the Web Security Appliance will communicate. |
| **Generate a certificate and key** | **a.** Select **Use Generated Certificate and Key**.<br>**b.** Click **Generate New Certificate and Key**.<br>**1.** In the Generate Certificate and Key dialog box, enter the information to display in the signing certificate.<br>**Note** You can enter any ASCII character except the forward slash ( / ) in the Common Name field.<br>**2.** Click **Generate**.<br>**c.** Click **Download Certificate** to transfer the certificate to the SaaS applications with which the Web Security Appliance will communicate.<br>**d.** (Optional) To use a signed certificate, click the **Download Certificate Signing Request** (DCSR) link to submit a request 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**. (bug 37984) |

**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.

**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.

**Step 8** Submit and Commit Changes.

### What to do next

After specifying the certificate and key to use for signing SAML assertions, upload the certificate to each SaaS application.

### Related Topics

- Configuring End-user Access to the Single Sign-on URL, on page 146

# Using SaaS Access Control and Multiple Appliances

### Before you begin

Configuring the Appliance as an Identity Provider, on page 142

### Procedure

**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 **Network > 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, on page 142.
- Provide an Identity Provider Signing Certificate and Key: Network > Identity Provider for SaaS > Enable and Edit Settings.
- Create an Authentication Realm, Authentication Realms, on page 99.

### Procedure

**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. |
| Metadata for Service Provider | 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.<br><br>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.<br><br>**Configure Keys Manually** – If you select this option, provide the following:<br><br>• **Service Provider Entity ID**. Enter the text (typically in URI format) the SaaS application uses to identify itself as a service provider.<br><br>• **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.<br><br>• **Assertion Consumer Service URL**. Enter the URL to which the Web Security Appliance is to send the SAML assertion it creates. Read the SaaS application documentation to determine the correct URL to use (also known as the login URL).<br><br>**Import File from Hard Disk** – If you select this option, click Browse, locate the file, and then click **Import**.<br><br>**Note**<br>This 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. |
| User Identification / Authentication for SaaS SSO | Specify how users are identified/authenticated for SaaS single sign-on:<br><br>• Always prompt users for their local authentication credentials.<br><br>• Prompt users for their local authentication credentials if the Web Proxy obtained their user names transparently.<br><br>• Automatically sign in SaaS users using their local authentication credentials.<br><br>Choose the authentication realm or 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. If an Identity Services Engine is used for authentication, and LDAP was selected, the realm will be used for the SAML user names and attribute mapping. |

| Property | Description |
|---|---|
| SAML User Name Mapping | 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:<br>• **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.<br>• **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 in the **Expression Name** field, with %s either before or after the string to indicate its position in the internal user name. |
| 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 | Choose the authentication mechanism the Web Proxy uses to authenticate its internal users.<br>**Note**<br>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.

### What to do next

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 SSO URL format is:

http://*IdentityProviderDomainName* /SSOURL/*ApplicationName*

### Procedure

**Step 1** Obtain the single sign-on URL from the **Web Security Manager > SaaS Policies** page.

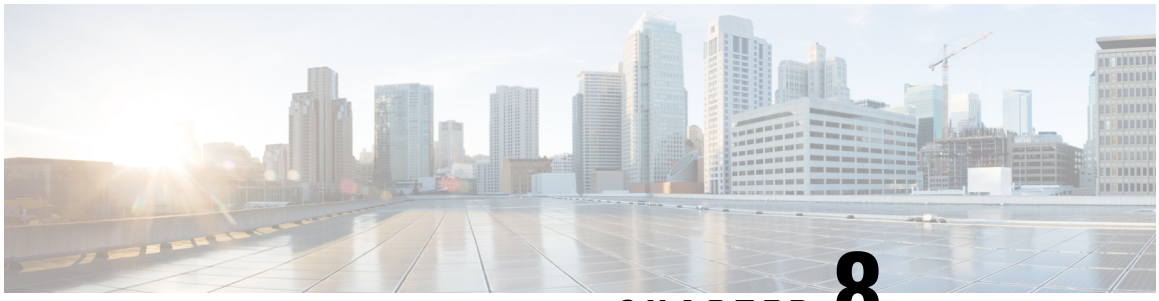
**Step 2** Make the URL available to end-users depending on which flow type.

**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 8

# Integrate the Cisco Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC)

This topic contains the following sections:


- Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service, on page 149
- ISE/ISE-PIC Certificates, on page 151
- Fallback Authentication, on page 152
- Tasks for Integrating the ISE/ISE-PIC Service, on page 153
- Configure ISE-SXP Integration, on page 160
- VDI (Virtual Desktop Infrastructure) User Authentication in ISE/ISE-PIC Integrations, on page 163
- Troubleshooting Identity Services Engine Problems, on page 163


## Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service

Cisco's Identity Services Engine (ISE), and Passive Identity Connector (ISE-PIC) are applications that run on separate servers in your network to provide enhanced identity management. The Web Security Appliance can access user-identity information from an ISE or ISE-PIC server. When either ISE, or ISE-PIC is configured, information is retrieved (user names and associated Secure Group Tags from ISE, user names and Active Directory groups from ISE-PIC) for appropriately configured Identification Profiles, to allow transparent user identification in policies configured to use those profiles.

- You can construct access policies using Secure Group Tags and Active Directory groups.
- For users that fail transparent identification with ISE/ISE-PIC, you can configure fallback authentication with Active Directory based realms. See Fallback Authentication, on page 152.
- You can configure authentication of users in Virtual Desktop Environments (Citrix, Microsoft shared/remote desktop services etc.). See VDI (Virtual Desktop Infrastructure) User Authentication in ISE/ISE-PIC Integrations, on page 163.

**Note**

- The ISE/ISE-PIC service is not available in Connector mode.
- ISE/ISE-PIC version 2.4, and PxGrid version 2.0 are supported.
- The ISE configuration page in the Web Security Appliance 's web interface is used to configure ISE or ISE-PIC servers, upload certificates, and to connect to either ISE or ISE-PIC services. The steps to configure ISE or ISE-PIC are similar and the any details specific for ISE-PIC configurations have been mentioned where applicable.

For more information on Secure Web Appliance ISE version support matrix, see ISE Compatibility Matrix Information.

***Table 5: Web Security Appliance -ISE Scale Support Matrix***

| Models | Session Scale Without AD Group Enabled | Session Scale With AD Group Enabled | |
|---|---|---|---|
| - | Maximum Supported Active Sessions | Maximum Supported Active Sessions | Maximum Supported End Points<br>(AD group entries for each user, and end point in ISE database.) |
| S680*,S690,S695 | 200K | 125K | 400K |
| S380*,S390,S600V | 150K | 50K | 150K |
| S190,S195,S300V | 50K | 50K | 75K |
| S100V | 50K | 40K | 50K |

### Related Topics

- About pxGrid, on page 150
- About the ISE/ISE-PIC Server Deployment and Failover, on page 151

# About pxGrid

Cisco's Platform Exchange Grid (pxGrid) enables collaboration between components of the network infrastructure, including security-monitoring and network-detection systems, identity and access management platforms, and so on. These components can use pxGrid to exchange information via a publish/subscribe method.

There are essentially three pxGrid components: the pxGrid publisher, the pxGrid client, and the pxGrid controller.

- pxGrid publisher – Provides information for the pxGrid client(s).

- pxGrid client – Any system, such as the Web Security Appliance , that subscribes to published information; in this case, Security Group Tag (SGT), Active Directory groups, user-group, and profiling information.
- pxGrid controller – In this case, the ISE/ISE-PIC pxGrid node that controls the client registration/management and topic/subscription processes.

Trusted certificates are required for each component, and these must be installed on each host platform.

# About the ISE/ISE-PIC Server Deployment and Failover

A single ISE/ISE-PIC node set-up is called a standalone deployment, and this single node runs the Administration, and Policy Service. To support failover and to improve performance, you must set up multiple ISE/ISE-PIC nodes in a distributed deployment. The minimum required distributed ISE/ISE-PIC configuration to support ISE/ISE-PIC failover on your Web Security Appliance is:

- Two pxGrid nodes
- Two Administration nodes
- One Policy Service node

This configuration is referred to in the *Cisco Identity Services Engine Hardware Installation Guide* as a 'Medium-Sized Network Deployment'. Refer to the network deployments section in that installation guide for additional information.

### Related Topics

- ISE/ISE-PIC Certificates, on page 151
- Tasks for Integrating the ISE/ISE-PIC Service, on page 153
- Connect to the ISE/ISE-PIC Services, on page 155
- Troubleshooting Identity Services Engine Problems, on page 163

# ISE/ISE-PIC Certificates



**Note** This section describes the certificates necessary for an ISE/ISE-PIC connection. Tasks for Integrating the ISE/ISE-PIC Service, on page 153 provides detailed information about these certificates. Certificate Management, on page 533, provides general certificate-management information for AsyncOS.

A set of two certificates is required for mutual authentication and secure communication between the Web Security Appliance and each ISE/ISE-PIC server:

- **Web Appliance Client Certificate** – Used by the ISE/ISE-PIC server to authenticate the Web Security Appliance .
- **ISE pxGrid Certificate** – Used by the Web Security Appliance to authenticate an ISE/ISE-PIC server on port 5222 for Web Security Appliance -ISE/ISE-PIC data subscription (on-going publish/subscribe queries to the ISE/ISE-PIC server).

These two certificates can be Certificate Authority (CA)-signed or self-signed. AsyncOS provides the option to generate a self-signed Web Appliance Client Certificate, or a Certificate Signing Request (CSR) instead, if a CA-signed certificate is needed. Similarly, the ISE/ISE-PIC server provides the option to generate self-signed ISE/ISE-PIC pxGrid certificates, or CSRs instead if CA-signed certificates are needed.

### Related Topics

- Using Self-signed Certificates, on page 152
- Using CA-signed Certificates, on page 152
- Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service, on page 149
- Tasks for Integrating the ISE/ISE-PIC Service, on page 153
- Connect to the ISE/ISE-PIC Services, on page 155

## Using Self-signed Certificates

When self-signed certificates are used on the ISE/ISE-PIC server, the ISE/ISE-PIC pxGrid certificate developed on the ISE/ISE-PIC server, as well as the Web Appliance Client Certificate developed on the Web Security Appliance must be added to the Trusted Certificates store on the ISE/ISE-PIC server (On **ISE** - Administration > Certificates > Trusted Certificates > Import; on **ISE-PIC** - Certificates > Trusted Certificates > Import).

## Using CA-signed Certificates

In the case of CA-signed certificates:

- On the ISE/ISE-PIC server, ensure the appropriate CA root certificate for the Web Appliance Client Certificate is present in the Trusted Certificates store (Administration > Certificates > Trusted Certificates).
- On the Web Security Appliance , ensure the appropriate CA root certificates are present in the Trusted Certificates list (Network > Certificate Management > Manage Trusted Root Certificates).
- On the Identity Services Engine page (Network > Identity Services Engine), be sure to upload the CA root certificate for the ISE/ISE-PIC pxGrid certificate.

# Fallback Authentication

For user information not available in ISE/ISE-PIC, you can configure a fallback authentication. Ensure you have the following for successful fallback authentication.

- Identification profile configured with a fallback option of Active Directory based realm.
- Access policy with the correct Identification profile which contains the fallback option.

# Tasks for Integrating the ISE/ISE-PIC Service

**Note**

- ISE/ISE-PIC version 2.4, and PxGrid version 2.0 are supported.
- To continue using existing access policies with ISE-PIC, you must edit the respective identification profiles to use ISE-PIC and identify users transparently. This applies to identification profiles using CDA. If you are migrating from CDA identification, to ISE-PIC based identification, you must edit the respective identification profiles.

**Note**

- Reconfigure the ISE on the Web Security Appliance , if you are upgrading from AsyncOS 11.5 or earlier versions to AsyncOS 11.7 or later versions.
- The certificate must be generated through the ISE/ISE-PIC device and the generated certificate must be uploaded to the Web Security Appliance .

| Step | Task | Links to Topics and Procedures |
|---|---|---|
| 1 | Generate certificate through ISE/ISE-PIC device | Generating Certificate through ISE/ISE-PIC, on page 154 |
| 2 | Configure the ISE/ISE-PIC for Web Security Appliance access. | Configuring ISE/ISE-PIC server for Web Security Appliance Access, on page 154 |
| 3 | Configure and enable ISE/ISE-PIC Services in the Web Security Appliance . | Connect to the ISE/ISE-PIC Services, on page 155 |
| 4 | If the Web Security Appliance Client Certificate is self-signed, import it to ISE/ISE-PIC. | Import the Self-signed Web Security Appliance Client Certificate to ISE/ISE-PIC Standalone Deployment, on page 157<br>Import the Self-signed Web Security Appliance Client Certificate to ISE/ISE-PIC Distributed Deployment, on page 158 |
| 5 | If required, configure logging in the Web Security Appliance . | Configuring logging for ISE/ISE-PIC, on page 159 |
| 6 | Acquire ISE/ISE-PIC ERS server details. | Acquiring ISE/ISE-PIC ERS Server Details from ISE/ISE-PIC, on page 160 |

### Related Topics

- Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service, on page 149
- ISE/ISE-PIC Certificates, on page 151
- Troubleshooting Identity Services Engine Problems, on page 163

# Generating Certificate through ISE/ISE-PIC

**Note** The certificate that is generated through the ISE/ISE-PIC device must be in the PKCS12 format.

- **ISE/ISE-PIC:**

### Procedure

**Step 1** Choose **Work Centres** > **PassiveID** > **Subscribers** > **Certificates**.

**Step 2** Choose **PKCS 12 format** from the **Certificate Download Format** drop-down list. Enter other appropriate information on the **Certificates** tab and generate a pxGrid certificate.

**Step 3** Extract Root CA, Web Appliance Client Certificate, and Web Appliance Client Key from the generated XXX.pk12 file using the `openssl` command:

- **Root CA:** openssl pkcs12 -in XXX.p12 -cacerts -nokeys -chain -out RootCA.pem
- **Web Appliance Client Certificate:** openssl pkcs12 -in XXX.p12 -clcerts -nokeys -out publicCert.pem
- **Web Appliance Client Key:** openssl pkcs12 -in XXX.p12 -nocerts -nodes -out privateKey.pem

**Note**
Use the same certificate password that you have entered on the ISE web interface while performing step 2.

**Note**
Follow the same steps to generate the secondary Root CA, Web Appliance Client Certificate, and Web Appliance Client Key through the secondary/failover ISE server.

# Configuring ISE/ISE-PIC server for Web Security Appliance Access

- **ISE**
  - Each ISE server must be configured to allow identity topic subscribers (such as Web Security Appliance ) to obtain session context in real-time.
    1. Choose **Administration** > **pxGrid Services** > **Settings** > **pxGrid Settings**.
    2. Ensure **Automatically approve new certificate-based accounts** is checked.

Delete any old Web Security Appliance s configured that do not take part in any authentication with ISE/ISE-PIC.

Ensure the ISE server footer is green, and says **Connected to pxGrid**.

- **ISE-PIC**
  - Each ISE-PIC server must be configured to allow identity topic subscribers (such as Web Security Appliance ) to obtain session context in real-time.
    1. Choose **Subscribers** > **Settings**.
    2. Ensure **Automatically approve new certificate-based accounts** is checked.

    Delete any old Web Security Appliance s configured that do not take part in any authentication with ISE/ISE-PIC.

    Ensure the ISE server footer is green, and says **Connected to pxGrid**.

Refer to Cisco *Identity Services Engine* documentation for more information.

# Connect to the ISE/ISE-PIC Services

**Note** If the ISE Admin, pxGrid, and MNT certificates are signed by your Root CA certificate, then upload the Root CA certificate itself to the ISE pxGrid Node Certificate fields on the appliance (**Network** > **Identity Services Engine**).

### Before you begin

- Be sure each ISE/ISE-PIC server is configured appropriately for Web Security Appliance access; see Tasks for Integrating the ISE/ISE-PIC Service, on page 153.
- Obtain valid ISE/ISE-PIC-related certificates and keys. See Generating Certificate through ISE/ISE-PIC, on page 154for related information.
- Import the obtained RootCA.pem to the Web Security Appliance (**Network** > **CertificateManagement** > **TrustedRootCertificate** > **Client on ManageTrustedRootCertificate**). To extract Root CA, Web Appliance Client Certificate, and Web Appliance Client Key from the generated XXX.pk12 file, see Generating Certificate through ISE/ISE-PIC, on page 154.

**Note** Follow the same procedure for RootCA.pem extracted from secondary XXXX.pk12 file (if secondary/failover ISE Sever is available).

- The ISE configuration page in the Web Security Appliance 's web interface is used to configure ISE or ISE-PIC servers, upload certificates, and to connect to either ISE or ISE-PIC services. The steps to configure ISE or ISE-PIC are identical, and any details specific to ISE-PIC configurations have been mentioned where applicable.
- Enable ERS if you are building access policies using Active Directory groups provided by ISE/ISE-PIC.

### Procedure

**Step 1** Choose **Network > Identification Service Engine**.

**Step 2** Click **Edit Settings**.

If you are configuring ISE/ISE-PIC for the first time, click **Enable and Edit Settings**.

**Step 3** Check **Enable ISE Service**.

**Step 4** Identify the **Primary Admin Node** using its host name or IPv4 address and provide the following information on the **Primary ISE pxGrid Node Tab** on the Web Security Appliance .

a) Provide an **ISE pxGrid Node Certificate** for Web Security Appliance -ISE/ISE-PIC data subscription (on-going queries to the ISE/ISE-PIC server).

Browse to and select the certificate (or the certificate chain that includes any intermediate certificates) which is generated from the primary ISE server as Root CA (i.e. RootCA.pem); see ,Generating Certificate through ISE/ISE-PIC, on page 154 and then click **Upload File**. See Uploading a Certificate and Key, on page 536 for additional information.

**Step 5** If you are using a second ISE/ISE-PIC server for failover, identify its **Primary Admin Node** using its host name or IPv4 address and provide the following information on the **Secondary ISE pxGrid Node** tab on the Web Security Appliance using its host name or IPv4 address.

a) Provide the secondary **ISE pxGrid Node Certificate**.

Browse to and select the certificate (or the certificate chain that includes any intermediate certificates) which is generated from the secondary ISE server as Root CA (i.e. **RootCA.pem**); see Generating Certificate through ISE/ISE-PIC, on page 154, and then click **Upload File** .See Uploading a Certificate and Key, on page 536 for additional information.

**Note**
During failover from primary to secondary ISE servers, any user not in the existing ISE SGT cache will be required to authenticate, or will be assigned Guest authorization, depending on your Web Security Appliance configuration. After ISE failover is complete, normal ISE authentication resumes.

**Step 6** Provide a **Web Appliance Client Certificate** for Web Security Appliance -ISE/ISE-PIC server mutual authentication:

- **Use Uploaded Certificate and Key**

  For both the certificate and the key, click Choose and browse to the respective file.

  **Note**
  Select and upload publicCert.pem and privateKey.pem generated through the ISE/ISE-PIC device. See Generating Certificate through ISE/ISE-PIC, on page 154.

  If the **Key is Encrypted**, check this box.

  Click **Upload Files**. (See Uploading a Certificate and Key, on page 536 for additional information about this option.)

**Step 7** Enable the ISE SGT eXchange Protocol (SXP) service.

For information on enabling Web Security Appliance to retrieve SXP binding topics from ISE services, see Enabling ISE-SXP Protocol for SGT-to-IP Address Mapping, on page 161.

**Step 8** Enable the ISE External Restful Service (ERS).

- Enter the username and password of the ERS administrator. SeeAcquiring ISE/ISE-PIC ERS Server Details from ISE/ISE-PIC, on page 160.
- If ERS is available on the same ISE/ISE-PIC pxGrid nodes, check the **Server name same as ISE pxGrid Node** check box. Otherwise, enter the primary and secondary (if configured), servers' hostnames or IPv4 addresses.

**Step 9** Click **Start Test** to test the connection with the ISE/ISE-PIC pxGrid node(s).

**Step 10** Click **Submit**.

### What to do next

- Classifying Users and Client Software, on page 131
- Create Policies to Control Internet Requests, on page 213

### Related Information

- http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html , particularly “How To Integrate Cisco Web Security Appliance  using ISE/ISE-PIC and TrustSec through pxGrid..”

# Import the Self-signed Web Security Appliance Client Certificate to ISE/ISE-PIC Standalone Deployment

The basic steps are:

- **ISE Admin Node**
  - Choose **Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

  Ensure that the following options are checked:
  - Trust for Authentication within ISE
  - Trust for client authentication and syslog
  - Trust for authentication of Cisco services
- **ISE-PIC Admin Node**
  - Choose **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

    Ensure that the following options are checked:
    - Trust for Authentication within ISE
    - Trust for client authentication and syslog
    - Trust for authentication of Cisco services

Refer to Cisco *Identity Services Engine* documentation for more information.

# Import the Self-signed Web Security Appliance Client Certificate to ISE/ISE-PIC Distributed Deployment

The basic steps are:

- **ISE Admin Node:**
  - Choose **Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

  Ensure that the following options are checked:
  - Trust for Authentication within ISE
  - Trust for client authentication and syslog
  - Trust for authentication of Cisco services
- **ISE-PIC Admin Node:**
  - Choose **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import**.

    Ensure that the following options are checked:
    - Trust for Authentication within ISE
    - Trust for client authentication and syslog
    - Trust for authentication of Cisco services

Refer to Cisco *Identity Services Engine* documentation for more information.

**Note** In Distributed ISE Deployment, the Web Security Appliance communicates with MNT, PAN, and PxGrid nodes. In this case, the certificates or the issuer for all of the certificates, must be available in the 'Extracted Root certificate' i.e. in the RootCA which is generated through the ISE/ISE-PIC device. See Generating Certificate through ISE/ISE-PIC, on page 154.

## Procedure

**Step 1** Follow the steps in the Generating Certificate through ISE/ISE-PIC, on page 154 to generate RootCA, Web Appliance Client Certificate, and Web Appliance Client Key.

**Step 2** On **ISE/ISE-PIC Admin Node**, export the self-signed certificates manually through **ISE/ISE-PIC** > **Administration** > **System** > **Certificates** > **System Certificates**

**a.** Select a certificate which is having 'Used by' one of these:[pxGrid, EAP Authentication, Admin, Portal, RADIUS DTLS].

**b.** Click **Export** and save the generated .pem file.

Repeat the above steps for all ISE/ISE-PIC distributed nodes.

**Step 3** Append the downloaded certificate-files in RootCA.pem manually using `openssl` commands. To generate and extract certificate-files in RootCA.pem through the ISE/ISE-PIC device, see Generating Certificate through ISE/ISE-PIC, on page 154.

**a.** Execute the following command on the downloaded certificate:

```
Example:

openssl x509 -in <DownloadCertificate>.pem -text | egrep "Subject:|Issuer:

Example (output):

Issuer: CN=isehcamnt2.node
Subject: CN=isehcamnt2.node
```

**b.** Modify the content as follows:

```
Example:
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

**c.** Add the following line in the RootCA.pem:

```
Bag Attributes: <Empty Attributes>
```

**d.** Add Subject and Issuer from step (2) in RootCA.pem along with step (3).

```
Example:
Bag Attributes: <Empty Attributes>
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

**e.** Copy the whole content of the downloaded certificate file and paste them at the end of the RootCA after step (4) data.

Repeat steps (1) to (5) for all Distributed ISE/ISE-PIC node downloaded certificates and save the modified RootCA certificate.

**Step 4** Upload the modified RootCA.pem in the ISE configuration page of the Web Security Appliance . See Connect to the ISE/ISE-PIC Services, on page 155.

# Configuring logging for ISE/ISE-PIC

- Add the custom field %m to the Access Logs to log the Authentication mechanism—Customizing Access Logs, on page 460.
- Verify that the ISE/ISE-PIC Service Log was created; if it was not, create it—Adding and Editing Log Subscriptions, on page 432.
- Define Identification Profiles that access ISE/ISE-PIC for user identification and authentication—Classifying Users and Client Software, on page 117.
- Configure access policies that utilize ISE/ISE-PIC identification to define criteria and actions for user requests—Policy Configuration, on page 191.

# Acquiring ISE/ISE-PIC ERS Server Details from ISE/ISE-PIC

- Enable the Cisco ISE REST API in ISE/ISE-PIC (the APIs use HTTPS port 9060).



**Note** You must enable ISE External Restful Service (ERS) on the Web Security Appliance (Network > Identity Services Engine) to configure security policies based on groups. This is applicable to 11.7 and later versions.

  - **ISE**
    - Choose **Administration** > **Settings** > **ERS Settings** > **ERS settings for primary admin node** > **Enable ERS**.

      Enable **ERS for Read for All Other Nodes** if there are any secondary nodes.
  - **ISE-PIC**
    - Choose **Settings** > **ERS Settings** > **Enable ERS**.

- Ensure you have created an ISE administrator with the correct External RESTful Services group. The External RESTful Services Admin group has full access to all ERS APIs (GET, POST, DELETE, PUT). This user can Create, Read, Update, and Delete ERS API requests. The External RESTful Services Operator has Read Only access (GET request only).
  - **ISE**
    - Choose **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users**.
  - **ISE-PIC**
    - Choose **Administration** > **Admin Access** > **Admin Users**.

If the ERS service is available on separate servers, and not on the ISE/ISE-PIC pxGrid nodes, you will need the primary and secondary (if configured), servers' hostnames or IPv4 addresses.

Refer to Cisco *Identity Services Engine* documentation for more information.

# Configure ISE-SXP Integration

This section includes the following topics:


- About ISE-SXP Protocol for SGT-to-IP Address Mapping, on page 161
- Guidelines and Limitations, on page 161
- Prerequisites, on page 161
- Enabling ISE-SXP Protocol for SGT-to-IP Address Mapping, on page 161
- Verifying the ISE-SXP Protocol Configuration, on page 162

# About ISE-SXP Protocol for SGT-to-IP Address Mapping

SGT Exchange Protocol (SXP) is a protocol developed to propagate the IP-SGT bindings across network devices. A Security Group Tag (SGT) specifies the privileges of a traffic source within a trusted network.

You can integrate Cisco Identity Services Engine (ISE) deployment with CiscoWeb Security Appliance for passive authentication. Web Security Appliance can subscribe to SXP mappings from ISE. ISE uses SXP to propagate the SGT-to-IP address mapping database to managed devices. When you configure Web Security Appliance to use the ISE server, you enable the option to listen to the SXP topic from ISE. This causes Web Security Appliance to learn about the SGTs and IP address mappings directly from ISE.

Web Security Appliance generates a dummy user authentication IP addresses, which include the ISE cluster IP address along with the IP address of the client. Therefore, multiple client IP addresses can be authenticated on the cluster IP address.

# Guidelines and Limitations

ISE-SXP protocol for SGT-to-IP address mapping has the following guidelines and limitations:

- IPv6 enabled endpoints are not support in Web Security Appliance Release 12.7.
- In Web Security Appliance Release 12.7, usernames and group mapping are not available in the SGT-to-IP address mappings. Therefore, the administrator cannot create policies based on ISE users and groups in Web Security Appliance . However, it can be created with SGTs.
- To schedule the restart timestamp for the bulk download process, you must configure time in the HH::MM format within 24 hours to restart the ised process.

**Note** It is recommended that you configure the time when the user authentication process is indicated to be less in the day. For example, at 00:00 hour.

# Prerequisites

ISE-SXP protocol for SGT-to-IP address mapping has the following prerequisite:

- Requires a trusted root certificate. To add a trusted root certificate, see Managing Trusted Root Certificates.

# Enabling ISE-SXP Protocol for SGT-to-IP Address Mapping

All mappings that are defined in ISE, including the SGT-to-IP address mappings can be published through SXP. You can retrieve the ISE-SXP information using the following mechanisms:

- Bulk download—After a ised process restart, Web Security Appliance sends the bulk download request to the ISE aggregator node in order to get information for all ISE-SXP entries that are available on the aggregator node. You can schedule the restart timestamp using AsyncOS Command Line Interface (CLI).
- Incremental update—Web Security Appliance subscribes over a websocket to get incremental update messages. There are two types of messages:
  - Create—for all newly created entries

- Delete—for all SXP updated entries

**Note** Web Security Appliance receives two messages (Delete followed by Create) for each entry that is updated.

You are allowed to schedule restart.

**Procedure**

**Step 1** Navigate to **Network** > **Identification Service Engine**.

**Step 2** Click **Edit Settings**.

**Step 3** Check **Enable ISE Service**.

**Step 4** Check **Enable** to enable Web Security Appliance to retrieve SXP binding topics from ISE services.

By default, the ISE SGT eXchange Protocol (SXP) service is disabled.

**Step 5** Click **Start Test** to test the connection.

**Note**
The SXP information is displayed only if the ISE-SGT eXchange Protocol (SXP) service has been enabled.

**Step 6** Click **Submit**.

# Verifying the ISE-SXP Protocol Configuration

You can verify the ISE-SXP protocol configuration using any one of the following methods:

- Click **Start Test** in the Enabling ISE-SXP Protocol for SGT-to-IP Address Mapping, on page 161 and verify the displayed information.
- Use the **STATISTICS** command under the **ISEDATA** command in the AsyncOS Command Line Interface (CLI).

When you use the **STATISTICS** command, the following information appears:

- ERS Hostname
- ERS Time of Connection
- Session Bulk Download
- Group Bulk Download
- SGT Bulk Download
- SXP Bulk Download
- Session Update

- Group Update
- SXP Update
- Memory Allocation
- Memory Deallocation
- Total Session Count

The user name is generated in the following format:

```
isesxp_<ISE-node-ip>_sgt<SGT number>_<Client IP address>
```

For example: isesxp_10.10.2.68_sgt18_10.10.10.10

# VDI (Virtual Desktop Infrastructure) User Authentication in ISE/ISE-PIC Integrations

You can configure transparent identification with ISE/ISE-PIC for users on VDI environments based on the source ports used.

You must install the Cisco Terminal Services (TS) Agent, on the VDI servers. The Cisco TS agent provides the identity information to ISE/ISE-PIC. The identity information includes domain, user name, and the port ranges used by each user.

- Download the Cisco TS agent from the support site https://www.cisco.com/c/en/us/support/index.html.
- See the Cisco Terminal Services (TS) Agent Guide https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html for more information.
- Configure the ISE/ISE-PIC API provider to work with a Cisco TS agent. See the Cisco TS agent documentation for information about sending API calls.

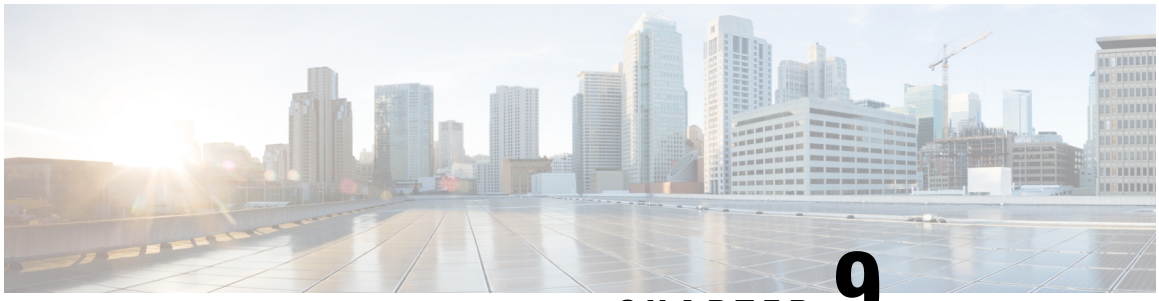


**Note**

- Fallback authentication for VDI environment users is not supported.
- Ensure the number of maximum remote desktop sessions are the same in the Cisco Terminal Services agent and Microsoft server settings. This prevents incorrect session information from being sent to the Web Security Appliance from ISE, and avoids false authentication for new sessions.

# Troubleshooting Identity Services Engine Problems

- Identity Services Engine Problems, on page 565
  - Tools for Troubleshooting ISE Issues, on page 565
  - ISE Server Connection Issues, on page 566
  - ISE-related Critical Log Messages, on page 568



CHAPTER 9

# Classify URLs for Policy Application

This topic contains the following sections:


- Overview of Categorizing URL Transactions, on page 165
- Configuring the URL Filtering Engine , on page 168
- Managing Updates to the Set of URL Categories , on page 168
- Filtering Transactions Using URL Categories, on page 175
- YouTube Categorization, on page 181
- Creating and Editing Custom URL Categories, on page 183
- Filtering Adult Content, on page 189
- Redirecting Traffic in the Access Policies, on page 191
- Warning Users and Allowing Them to Continue, on page 192
- Creating Time Based URL Filters, on page 193
- Viewing URL Filtering Activity, on page 194
- Regular Expressions, on page 195
- URL Category Descriptions, on page 198


## 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, on page 167 |
| Control access to HTTP, HTTPS, and FTP requests | Filtering Transactions Using URL Categories, on page 175 |
| Create user defined custom URL categories that specify specific hostnames and IP addresses | Creating and Editing Custom URL Categories, on page 183 |

# 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



**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.

### Procedure

**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.

# 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, on page 194.
- Creating and Editing Custom URL Categories, on page 183.

# 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.

To see what category a particular web site is assigned to, go to the URL in Reporting Uncategorized and Misclassified URLs, on page 167.

### Related Topics

- Uncategorized URLs, on page 166.

# 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://talosintelligence.com/tickets
  - 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.
- https://www.talosintelligence.com/reputation_center/support
  - To submit a dispute, you must be logged into your Cisco account. Disputes can be filed for URLs, IPs, or domains.
  - Use the Reputation Center Search box to look up web reputation information.

# 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.

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.

To see what category a particular web site is assigned to, go to the URL in Reporting Uncategorized and Misclassified URLs, on page 167.

### Related Topics

- Manually Updating the URL Category Set , on page 173

# Configuring the URL Filtering Engine

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

### Procedure

**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 any one of the following Cisco Web Usage Controls:

**a.** Application Visibility and Control

**b.** Dynamic Content Analysis Engine

**c.** Multiple URL Categories

**Note**
The Multiple URL Categories feature is applicable only for Access Policies. You cannot apply the Multiple URL Categories feature for decryption policies and identification profiles.

**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<br>(Do these tasks as part of your initial setup) | Understanding the Impacts of URL Category Set Updates , on page 169<br>Controlling Updates to the URL Category Set , on page 172<br>Default Settings for New and Changed Categories , on page 173<br>Receiving Alerts About Category and Policy Changes , on page 174 |
| After updates occur | Responding to Alerts about URL Category Set Updates , on page 174 |

# 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 , on page 169
- Effects of URL Category Set Updates on Filtering Actions in Policies , on page 169

## 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 the new URL categories now, one of the following actions will be picked from the Default Action for Update Categories option of the Policy Configuartion page:<br>• Least Restrictive<br>• Most Restrictive<br>The actions are set by default for the new categories. In Access Policies, and Cisco Data Security Policies:<br>• Most Restrictive is Block<br>• Least Restrictive is Monitor<br>In Web Traffic Tap (WTT) Policies:<br>• Most Restrictive is Tap<br>• Least Restrictive is No Tap<br>In Decryption Policies:<br>• Most Restrictive is Block<br>• Least Restrictive is Pass Through |
| A category can be deleted | The action associated with the deleted category is deleted.<br>If the policy depended exclusively on the deleted category, the policy is disabled.<br>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. New category actions will be picked from the Default Action for Update Categories. |

| Change | Effect on Policies and Identities |
|---|---|
| Two or more existing categories can merge | 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.”<br><br>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:<br><br>• 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.<br><br>• 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.<br><br>In this case, sites that were previously blocked may now be accessible to users.<br><br>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.<br><br>The order of restrictiveness is as follows (not all actions are available for all policy types):<br><br>• Block<br><br>• Drop<br><br>• Decrypt<br><br>• Warn<br><br>• Time-based<br><br>• Monitor<br><br>• Pass Through<br><br>**Note**<br>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.) |

### Related Topics

• Merged Categories - Examples , on page 172.

# 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<br>Use the least restrictive among the original categories. | Warn |
| Monitor | • Block or<br>• Use Global Settings,when Global is set to Block | • Block or<br>• Use Global Setting, when Global is set to Block<br>Use the most restrictive among the original categories. | Block |
| Block | • Monitor or<br>• Use Global Settings, when Global is set to Monitor | • Monitor or<br>• Use Global Setting, when Global is set to Monitor<br>Use the least restrictive among the original categories. | Monitor |
| For policies in which membership is defined by URL category:<br>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 , on page 173<br>and<br>Manually Updating Security Service Components, on page 541 |
| Disabling all automatic updates | Configuring Upgrade and Service Update Settings, on page 545. |

**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.

### Procedure

**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 **Default Action for Update Categories** setting in that policy.

## Verifying Existing Settings and/or Making Changes

### Procedure

**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.

### What to do next

### Related Topics

- Effects of URL Category Set Updates on Filtering Actions in Policies , on page 169.

# 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.

### Procedure

**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 , on page 169

# Filtering Transactions Using URL Categories

The URL filtering engine lets you 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, on page 175 |
| Decryption Policies | Configuring URL Filters for Decryption Policy Groups, on page 178 |
| Cisco Data Security Policies | Configuring URL Filters for Data Security Policy Groups, on page 179 |

### Related Topics

- Redirecting Traffic in the Access Policies, on page 191
- Warning Users and Allowing Them to Continue, on page 192
- Creating and Editing Custom URL Categories, on page 183
- Effects of URL Category Set Updates on Filtering Actions in Policies , on page 169

# Configuring URL Filters for Access Policy Groups

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

### Procedure

**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:

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 included custom URL category.

| Action | Description |
|---|---|
| Use Global Settings | Uses the action for this category in the Global Policy Group. This is the default action for user defined policy groups.<br>Applies to user defined policy groups only.<br>**Note**<br>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. |
| Block | The Web Proxy denies 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.<br>Allowed requests bypass all further filtering and malware scanning.<br>Only use this setting for trusted web sites. You might want to use this setting for internal sites. |
| 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. |
| Quota-Based | As a individual user approaches either the volume or time quotas you have specified, a warning is displayed. When a quota is met, a block page is displayed. See Time Ranges and Quotas, on page 233. |
| Time-Based | The Web Proxy blocks or monitors the request during the time ranges you specify. See Time Ranges and Quotas, on page 233. |

**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
- Quota-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.

### What to do next

- Exceptions to Blocking for Embedded and Referred Content, on page 177

## Exceptions to Blocking for Embedded and Referred Content

A Website may embed or refer to content that is categorized differently than the source page, or that is considered an application. By default, embedded/referred content is blocked or monitored based on the action selected for its assigned category or application, regardless of how the source Website is categorized. For example, a *News* site could contain content, or a link to content, that categorized as *Streaming Video* and identified as being the application YouTube. According to your policy, *Streaming Video* and YouTube are both blocked, while *News* sites are not.

**Note** Requests for embedded content usually include the address of the site from which the request originated (this is known as the "referer" field in the request's HTTP header). This header information is used to determine categorization of the referred content.

You can use this feature to define exceptions to the default actions for embedded/referred content; for example, to permit all content embedded in or referred to from *News* Websites, or from a custom category representing your intranet.

**Note** Referer-based exceptions are supported only in Access policies. To use this feature with HTTPS traffic, before defining exceptions in Access policies, you must configure HTTPS decryption of the URL Categories that you will select for exception. See Configuring URL Filters for Decryption Policy Groups, on page 178 for information about configuring HTTPS decryption. See Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content, on page 564 for additional information about using this feature with HTTPS decryption.

### Procedure

**Step 1** On the URL Filtering page for a particular Access Policy (see Configuring URL Filters for Access Policy Groups, on page 175), click **Enable Exceptions** in the Exceptions to Blocking for Embedded/Referred Content section.

**Step 2** Click the **Click to select categories** link in the Set Exception for Content Referred by These Categories column, opening the URL filtering category referral-exception selection page.

**Step 3** From the Predefined and Custom URL Categories lists, select the categories for which you wish to define this referral exception, then click **Done** to return to the URL Filtering page for this Access Policy.

**Step 4** Choose an exception type from the Set Exception for this Referred Content drop-down list:

- **All embedded/referred content** – All content embedded in and referred from sites of the specified category types is not blocked, regardless of the categorization of that content.

- **Selected embedded/referred content** – After choosing this option, select specific Categories and Applications that are not blocked when originating from the specified URL categories.
- **All embedded/referred content except** – After choosing this option, all content embedded in and referred from sites of the specified category types is not blocked, except those URL categories and applications you now specify here. In other words, these types will remain blocked.

**Note**
The Referrer Exception option is enabled by default for the custom URL category even when this category is not included in Access Policies.

**Step 5** Submit and Commit Changes.

### What to do next

You can elect to display "Permitted by Referrer" transaction data in the tables and charts provided on the following Reporting pages: URL Categories, Users and Web Sites, as well as related charts on the Overview page. See Choosing Which Data to Chart , on page 357 for more information about selecting chart-display options.

# Configuring URL Filters for Decryption Policy Groups

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

### Procedure

**Step 1** Choose **Web Security Manager > Decryption 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:

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** 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.<br>Applies to user defined policy groups only.<br>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.

**Procedure**

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

**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:

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 | Uses the action for this category in the Global Policy Group. This is the default action for user defined policy groups.<br>Applies to user defined policy groups only.<br>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. |
| Allow | Always allows upload requests for web sites in this category. Applies to custom URL categories only.<br>Allowed requests bypass all further data security scanning and the request is evaluated against Access Policies.<br>Only use this setting for trusted web sites. You might want to use this setting for internal sites. |
| 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. |

**Note**
If you do not disable the maximum file size limitation, Web Security Appliance continues to validate the maximum file size when the Allow or Monitor options are selected in the URL filtering.

**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.

**What to do next**

**Related Topics**

• Effects of URL Category Set Updates on Filtering Actions in Policies , on page 169.

# YouTube Categorization

The YouTube categorization feature enables you to create a custom URL category for YouTube and set policies on the YouTube custom category for secure and control access.

**Note** When you configure the time-based access policy rules to block specific YouTube category:

- The time-based rules that you set are not applicable to the videos that are already opened and playing at the time when you configure the access policy.
- The rules will be applicable only to the videos that are newly opened after you set the rules.

**Note**

- Make sure that the googleapis.com is not blocked in upstream proxy or upstream firewall. If you have configured an exception for Cisco update server and WBNP telemetry server, configure the same for googleapis.com as well.
- You cannot block the video that appears on the main page of a channel, even if the video belongs to a blocked YouTube category.

  For example, you blocked autos and vehicles under YouTube category. If you open a video under the specified category on the main page of a channel related to autos and vehicles, the video will not be blocked. If you try to open the same video in a separate tab, it will be blocked as expected.

To configure the YouToube categorization feature, perform the following tasks.

| Step | Task | Links to Topics and Procedures |
|---|---|---|
| 1. | Create custom and external URL category for YouTube with www.youtube.com and m.youtube.com. | Creating and Editing Custom URL Categories, on page 183. |
| 2. | Add custom and external URL category for YouTube to a decryption policy. | Configuring URL Filters for Decryption Policy Groups, on page 178. |
| 3. | Enable YouTube categorization feature. | Enabling the YouTube Categorization Feature, on page 182. |
| 4. | Apply access policies to custom and external URL category for YouTube. | Configuring URL Filters for Access Policy Groups, on page 175.<br>**Note**<br>You must set the actions 'Block, Monitor, or Warn' under the YouTube Category Filtering section in the **Access Policies: URL Filtering** page. |

# Enabling the YouTube Categorization Feature

### Before you begin

- Enable HTTPS proxy (**Security Services** > **HTTPS Proxy**).
- Enable Acceptable Use Controls (**Security Services** > **Acceptable Use Controls**).
- Configure Custom and External URL categories (**Web Security Manager** > **Custom and External URL Categories**) with www.youtube.com and m.youtube.com.
- Configure decryption policy using the Custom and External URL category for YouTube, with action as 'decrypt'.
- Generated the Google API key using Google API services for YouTube. To generate Google API key:
  1. Logon to https://console.developers.google.com/ using Google account credentials. (Recommend not to use personal Google account).
  2. Create a project.
  3. In the **Enable APIs and Services**, enable **YouTube Data API v3.**
  4. Generate an API key using the wizard or use the **Credentials** option under **APIs & Services**.

**Note** If you are generating the API key using wizard, under **YouTube Data API v3**:

a. From the **Where will you be calling the API from?** drop-down list, choose **Other non-UI (e.g. cron job, daemon)** .

b. In the **What data will you be accessing** section, choose **Public data**.

c. Click **What credentials do I need?** then click **Done**.

### Procedure

**Step 1** Choose **Security Services** > **Acceptable Use Controls**.

**Step 2** Click **Edit Global Settings**.

**Step 3** Check the Enable checkbox next to YouTube categorization.

**Step 4** Enter the API key generated using the Google API services.

You must generate the API key using the Google API services before you enable the YouTube Categorization feature.

**Step 5** Enter the query timeout to set timeout period between the appliance and the YouTube API server.

**Step 6** Choose the routing table through which the YouTube category traffic passes through:

- Data : For P1 and P2 interfaces
- Management: For M1 interface

**Note**

The default routing table is data. The above two options are avaialble only if you have configured two separate routing tables for data and management services (Network > Interfaces).

**Step 7** Submit and commit your changes.

# Creating and Editing Custom URL Categories

You can create custom and external live-feed URL categories that describe specific host names 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 assign different actions to each category, the action of the higher included custom URL category takes precedence.



**Note** The number of external live feed files that can be used in these URL category definitions is limited to 30 and each file should contain no more than 5000 entries. Increasing external feed entries or having a large number of Regex entries causes performance degradation.

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 to parse the access logs. If the first four characters of the custom URL category include a space, Sawmill cannot properly parse the access log entry. Instead, only use supported characters in the first four characters. 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.



**Note** If DNS resolves several IPs to a website, and if one of those IPs is custom blocked list, then the Web Security Appliance blocks the website for all IPs, irrespective of they not being listed in the custom blocked list.

### Before you begin

Go to **Security Services** > **Acceptable Use Controls** to enable Acceptable Use Controls.

### Procedure

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

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

**Step 3** Provide the following information.

| Setting | Description |
|---|---|
| Category Name | Enter an identifier for this URL category. This name appears when you configure URL filtering for policy groups. |

| Setting | Description |
|---|---|
| List Order | Specify the order of this category in the list of custom URL categories. Enter "1" for the first URL category in the list.<br>The URL filtering engine evaluates a client request against the custom URL categories in the order specified. |
| Category Type | Choose **Local Custom Category** or **External Live Feed Category**. |
| Routing Table | Choose **Management** or **Data**. This choice is available only if "split routing" is enabled; that is, it is not available with local custom categories. See Enabling or Changing Network Interfaces, on page 24 for information about enabling split routing. |
| Sites / Feed File Location | If you choose **Local Custom Category** for the **Category Type**, provide the custom **Sites**:<br>• Enter one or more Site addresses for this custom category. You can enter multiple addresses separated by line breaks or commas. These addresses can be in any of the following formats:<br>  • IPv4 address, such as 10.1.1.0<br>  • IPv6 address, such as 2001:0db8::<br>  • IPv4 CIDR address, such as 10.1.1.0/24<br>  • IPv6 CIDR address, such as 2001:0db8::/32<br>  • Domain name, such as example.com<br>  • Hostname, such as crm.example.com<br>  • Partial hostname, such as .example.com; this will also match www.example.com<br>  • Regular expressions can be entered in the **Advanced** section, as described below.<br>**Note**<br>  •<br>  • It is possible to use the same address in multiple custom URL categories, but the order in which the categories are listed is relevant. If you include these categories in the same policy, and define different actions for each, the action defined for the category listed highest in the custom URL categories table will be the one applied.<br>• (Optional) Click **Sort URLs** to sort all addresses in the Sites field.<br>**Note**<br>Once you sort the addresses, you cannot retrieve their original order. |

| Setting | Description |
|---|---|
| Excluded Sites | If you choose **External Live Feed Category** for the **Category Type**, provide the sites that you want to exclude from the existing feed file. You can enter multiple addresses separated by line breaks or commas. These addresses can be in any of the following formats:<br>• IPv6 addresses such as 2001:0db8::/32<br>• IPv4 addresses such as 10.1.1.0.<br>• CIDR IPv6 addresses such as 2001:0db8::/32<br>• CIDR IPv4 address such as 10.1.1.0/24<br>• Domain name, such as example.com<br>• Hostname, such as crm.example.com<br>• Partial hostname, such as .example.com; will also match www.example.com |

| Setting | Description |
|---|---|
| Feed Location (cont.) | If you choose **External Live Feed Category** for the **Category Type**, provide the **Feed File Location** information; that is, locate and download the file containing the addresses for this custom category:<br>**a.** Select either **Cisco Feed Format**, or **Office 365 Feed Format**, or **Office 365 Web Service**, and provide the appropriate feed-file information.<br>• **Cisco Feed Format**:<br>• Choose the transport protocol to be used—either HTTPS or HTTP—and then enter the URL of the live-feed file. This file must be a comma-separated values (.csv)-formatted file. See External Feed-file Formats, on page 188 for more information about this file.<br>• Optionally, provide **Authentication** credentials in the **Advanced** section. Provide a Username and Passphrase to be used for connection to the specified feed server.<br>• **Office 365 Feed Format**:<br>• Enter the **Office 365 Feed Location** (URL) of the live-feed file.<br>This file must be an XML-formatted file; see External Feed-file Formats, on page 188 for more information about this file.<br>• **Office 365 Web Service**<br>Enter the web service URL. It must not contain a ClientRequestId, and have JSON as the format. The appliance automatically generates the ClientRequestId.<br>**b.** For Cisco Feed Format and Office 365 Feed formats, click **Get File** to test the connection to the feed server, and then parse and download the feed file from the server.<br>Progress is displayed in the text box below the **Get File** button. If an error occurs, the problem is indicated and must be rectified before trying again. Refer to Issues Downloading An External Live Feed File, on page 569 for additional information about possible errors.<br>For the Office 365 Web Service, click **Start Test** to initiate the service and download URLs and IPs.<br>**Note**<br>You can use no more than 30 External Live Feed files in these URL category definitions, and each file should contain no more than 5000 entries. Increasing the number of external feed entries causes performance degradation.<br>**Tip**<br>After you save your changes to this live-feed category, you can click **View** in the **Feed Content** column for this entry on the Custom and External URL Categories page (**Web Security Manager** > **Custom and External URL Categories**) to open a window that displays the addresses contained in the Cisco Feed Format or Office 365 Feed Format feed file you downloaded here. |

| Setting | Description |
|---|---|
| Advanced | If you choose **Local Custom Category** for the Category Type, you can enter regular expressions in this section to specify additional sets of addresses.<br>You can use regular expressions to specify multiple addresses that match the patterns you enter.<br>**Note**<br>• 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.<br>• Use "%20" instead of space character while adding URL paths as regular expressions. URL paths must not contain space characters when used as regular expressions.<br>•<br>See Regular Expressions, on page 195 for more information about using regular expressions. |
| Advanced (Exclude Regular Expresions) | If you choose **External Live Feed Category** for the **Category Type**, enter the regular expressions that you want to exclude from the existing feed file. Entries must exactly match the regular expressions existing in the feed file. |
| Auto Update the Feed | Choose a feed update option:<br>• **Do not auto update**<br>• **Every *n* HH:MM**; for example, enter 00:05 for five minutes. However, note that updating frequently can affect Web Security Appliance performance.<br>**Note**<br>Upon every reload and republish, the appliance downloads the available feed file and updates the downloaded time, even if the available feed file is same as the currently downloaded one. |

**Step 4** Submit and Commit Changes.

### What to do next

**Related Topics**

- Regular Expressions, on page 195.
- Customizing Access Logs, on page 460.
- Problems with Custom and External URL Categories, on page 568

# Address Formats and Feed-file Formats for Custom and External URL Categories

When Creating and Editing Custom and External URL Categories, you must provide one or more network addresses, whether for a **Local Custom Category**, or in an **External Live Feed Category** feed file. In each instance, you can enter multiple addresses separated by line breaks or commas. These addresses can be in any of the following formats:

- IPv4 address, such as 10.1.1.0
- IPv6 address, such as 2001:0db8::
- IPv4 CIDR address, such as 10.1.1.0/24
- IPv6 CIDR address, such as 2001:0db8::/32
- Domain name, such as example.com
- Hostname, such as crm.example.com
- Partial hostname, such as .example.com; this will also match www.example.com
- Regular expressions to specify multiple addresses that match the provided patterns (see Regular Expressions, on page 195 for more information about using regular expressions)



**Note** It is possible to use the same address in multiple custom URL categories, but the order in which the categories are listed is relevant. If you include these categories in the same policy, and define different actions for each, the action defined for the category listed highest in the custom URL categories table will be the one applied.

## External Feed-file Formats

If you select **External Live Feed Category** for the **Category Type** when Creating and Editing Custom and External URL Categories, you must select the feed format (**Cisco Feed Format** or **Office 365 Feed Format**) and then provide a URL to the appropriate feed-file server.

The expected format for each feed file is as follows:

- **Cisco Feed Format** – This must be a comma-separated values (.csv) file; that is, a text file with a .csv extension. Each entry in the .csv file must be on a separate line, formatted as address/comma/addresstype (for example: `www.cisco.com,site` or `ad2.*\.com`,regex). Valid addresstypes are `site` and `regex`. Here is an excerpt from a Cisco Feed Format .csv file:

```
www.cisco.com,site

\.xyz,regex

ad2.*\.com,regex

www.trafficholder.com,site

2000:1:1:11:1:1::200,site
```



**Note** Do not include `http://` or `https://` as part of any `site` entry in the file, or an error will occur. In other words, `www.example.com` is parsed correctly, while `http://www.example.com` produces an error.

- **Office 365 Feed Format** – This is an XML file located on a Microsoft Office 365 server, or a local server to which you saved the file. It is provided by the Office 365 service and cannot be modified. The network addresses in the file are enclosed by XML tags, following this structure: `products` > `product`

> `addresslist` > `address`. In the current implementation, an `addresslist` type can be IPv6, IPv4, or URL (which can include domains and regex patterns). Here is a snippet of an Office 365 feed file:

```
<products updated="4/15/2016">
   <product name="o365">
      <addresslist type="IPv6">
         <address>2603:1040:401::d:80</address>
         <address>2603:1040:401::a</address>
         <address>2603:1040:401::9</address>
      </addresslist>
      <addresslist type="IPv4">
         <address>13.71.145.72</address>
         <address>13.71.148.74</address>
         <address>13.71.145.114</address>
      </addresslist>
      <addresslist type="URL">
         <address>*.aadrm.com</address>
         <address>*.azurerms.com</address>
         <address>*.cloudapp.net2</address>
      </addresslist>
   </product>
   <product name="LYO">
      <addresslist type="URL">
         <address>*.broadcast.skype.com</address>
         <address>*.Lync.com</address>
      </addresslist>
   </product>
 </products>
```

# 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



**Note** When you enable Safe Search or Site Content Rating, the AVC Engine is tasked with identifying applications for safe browsing. As one of the criteria, the AVC engine will scan the response body to detect a search application. As a result, the appliance will not forward range headers.

### Procedure

**Step 1** Choose **Web Security Manager > Access Policies**.

**Step 2** Click the link under the URL Filtering 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.

### What to do next

### Related Topics

- Warning Users and Allowing Them to Continue, on page 192.

# 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. |
| encrt | 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, on page 445.

# 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.

### Procedure

**Step 1** Choose **Web Security Manager > Access Policies**.

**Step 2** Click the link under the URL Filtering 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.

#### What to do next

#### Related Topics

• Creating and Editing Custom URL Categories, on page 183

## 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

**Note**

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

### Procedure

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

**Step 4** Click Submit.

### What to do next

**Related Topics**

- Filtering Adult Content, on page 189
- Custom Messages on Notification Pages, on page 337
- Configuring the End-User URL Filtering Warning Page, on page 335

# Creating Time Based URL Filters

You can configure how the Web Security Appliance to 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.

### Procedure

**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** 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.

### What to do next

**Related Topics**

- Time Ranges and Quotas, on page 233

# 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, on page 353

# 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. |

# URL Category Logging in Access Logs

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, on page 425.
- URL Category Descriptions, on page 198.

# Regular Expressions

The Web Security Appliance uses a regular expression syntax that differs slightly from the regular expression syntax used by other Velocity pattern-matching engine implementations. Further, 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, simply type the forward slash without a backward slash.



**Note** Technically, AsyncOS for Web uses the Flex regular expression analyzer.

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. The maximum number of characters that can be used in regular expressions has been set to 2048 to restrict any web security vulnerability.
- **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, on page 183

# Forming Regular Expressions

Regular expressions are rules that typically use the word “matches” in the expressions. 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)
```



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

# Guidelines for Avoiding Validation Failures

**Important: Regular expressions that return more that 63 characters will fail and produce an invalid-entry error. Please be sure to form regular expressions that do not have the potential to return more than 63 characters.**

Follow these guidelines to minimize validation failures:

- Use literal expressions rather than wildcards and bracketed expressions whenever possible. A literal expression is essentially just straight text such as "`It's as easy as ABC123`". This is less likely to fail than using "`It's as easy as [A-C]{3}[1-3]{3}`". The latter expression results in the creation of non-deterministic finite automatons (NFA) entries, which can dramatically increase processing time.
- Avoid the use of an unescaped dot whenever possible. The dot is a special regular-expression character that means match any character except for a newline. If you want to match an actual dot, for example, as in "`url.com`", then escape the dot using the `\` character, as in "`url\.com`". Escaped dots are treated as literal entries and therefore do not cause issues.
- Any unescaped dot in a pattern that will return more than 63 characters after the dot will be disabled by the pattern-matching engine, and an alert to that effect will be sent to you, and you will continue to receive an alert following each update until you correct or replace the pattern.

  Similarly, use more specific matches rather than unescaped dots wherever possible. For example, if you want to match a URL that is followed by a single digit, use "`url[0-9]`" rather than "`url.`".
- Unescaped dots in a larger regular expression can be especially problematic and should be avoided. For example, "`Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created .qual`" may cause a failure. Replacing the dot in "`.qual`" with the literal "`equal`" should resolve the problem.

  Also, an unescaped dot in a pattern that will return more than 63 characters after the dot will be disabled by the pattern-matching engine. Correct or replace the pattern.
- You cannot use "`.*`" to begin or end a regular expression. You also cannot use "`./`" in a regular expression intended to match a URL, nor can you end such an expression with a dot.
- Combinations of wildcards and bracket expressions can cause problems. Eliminate as many combinations as possible. For example, "`id:[A-F0-9]{8}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{12}\) Gecko/20100101 Firefox/9\.0\.1\$`" may cause a failure, while "`Gecko/20100101 Firefox/9\.0\.1\$`"

will not. The latter expression does not include any wildcards or bracketed expressions, and both expressions use only escaped dots.

When wildcards and bracketed expressions cannot be eliminated, try to reduce the expression's size and complexity. For example, "`[0-9a-z]{64}`" may cause a failure. Changing it to something smaller or less complex, such as "`[0-9]{64}`" or "`[0-9a-z]{40}`" may resolve the problem.

If a failure occurs, try to resolve it by applying the previous rules to the wildcard (such as *, + and .) and bracketed expressions.



**Note** You can use the CLI option `advancedproxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex?` to enable or disable default regex conversion to lower case for case-insensitive matching. Use if you are experiencing issues with case sensitivity. See Web Security Appliance CLI Commands, on page 591 for more information about this option.

# Regular Expression Character Table

| Meta-character | Description |
|---|---|
| . | Matches any single character, except the newline character (0x0A). For example, the regular expression r.t matches the strings rat, rut, r t, but not root.<br>Be wary of using unescaped dots in long patterns, and especially in the middle of longer patterns. See Guidelines for Avoiding Validation Failures, on page 196 for more information. |
| * | Matches zero or more occurrences of the character immediately preceding. For example, the regular expression .* means match any string of characters, and [0-9]* matches any string of digits.<br>Be wary of using this meta-character, especially in conjunction with the dot character. Any pattern containing an unescaped dot that returns more than 63 characters after the dot will be disabled. See Guidelines for Avoiding Validation Failures, on page 196 for more information. |
| \ | The escape character; it means treat the following meta-character as an ordinary character. For example, \^ is used to match the caret character (^) rather than the beginning of a line. Similarly, the expression \. is used to match an actual dot rather than any single character. |
| ^ | Matches the beginning of a line. For example, the regular expression ^When in matches the beginning of the string "When in the course of human events" but not the string "What and when in the". |
| $ | Matches the end of a line or string. For example, b$\. matches any line or string that ends with "b." |
| + | Matches one or more occurrences of the character or regular expression immediately preceding. For example, the regular expression 9+ matches 9, 99, and 999. |

| Meta-character | Description |
|---|---|
| ? | Matches zero or one occurrence of the preceding pattern element. For example, colou?r matches both “colour” and “color” since the “u” is optional. |
| ( ) | Treat the expression between the left and right parens as a group, limiting the scope of other meta-characters. For example, (abc)+ matches one or more occurrences of the string “abc”; such as, “abcabcabc” or “abc123” but not “abab” or “ab123”. |
| \| | Logical OR: matches the preceding pattern or the following pattern. For example (him\|her) matches the line “it belongs to him” and the line “it belongs to her” but does not match the line “it belongs to them.” |
| [ ] | Matches any one of the characters between the brackets. For example, the regular expression r[aou]t matches “rat”, “rot”, and “rut”, but not “ret”.<br>Ranges of characters are specified by a beginning character, a hyphen, and an ending character. For example, the pattern [0-9] means match any digit. Multiple ranges can be specified as well. The pattern [A-Za-z] means match any upper- or lower-case letter. To match any character except those in the range (that is, the complementary range), use a caret as the first character after the opening bracket. For example, the expression [^269A-Z] matches any characters except 2, 6, 9, and uppercase letters. |
| { } | Specifies the number of times to match the previous pattern.<br>For example:<br>D{1,3} matches one to three occurrences of the letter D<br>Matches a specific number {**n**} or a minimum number {**n**,} of instances of the preceding pattern. For example, the expression A[0-9]{3} matches “A” followed by exactly three digits. That is, it matches “A123” but not “A1234”. The expression [0-9]{4,} matches any sequence of four or more digits. |
| “...” | Literally interpret any characters enclosed within the quotation marks. |

# 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<br>www.sincerelynot.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<br>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 Medicine." Bars and restaurants are classified as "Dining and Drinking." | www.samueladams.com<br>www.whisky.com |
| Animals and Pets | pets | 1107 | Information about domestic animals, livestock, service animals, pets and their care. Veterinary services, medicines, and animal health. Pet and animal training, aquariums, zoos, and animal shows. Includes animal shelters, humane societies, animal centric charities, and sanctuaries, bee keeping, training, and animal husbandry; dinosaurs and extinct animals. | www.petmd.com<br>www.wheatenorg.uk |
| 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<br>www.nga.gov |
| Astrology | astr | 1074 | Astrology; horoscope; fortune telling; numerology; psychic advice; tarot. | www.astro.com<br>www.astrology.com |
| Auctions | auct | 1088 | Online and offline auctions, auction houses, and classified advertisements. | www.craigslist.com<br>www.ebay.com |

| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| 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<br>www.ge.com |
| Cannabis | cann | 1109 | Websites that focus on the recreational and medicinal consumption of cannabis. Sites may include marketing, discussions about legal and regulatory issues, growth and production, paraphernalia, research, and investment in the cannabis industry. Dispensaries, cannabinoid (CBD oil, THC, etc.) based products are also included. | www.localproduct.co<br>www.oregonbc.com |
| Chat and Instant Messaging | chat | 1040 | Web-based instant messaging and chat rooms. | www.icq.com<br>www.e-chat.co |
| Cheating and Plagiarism | plag | 1051 | Promoting cheating and selling written work, such as term papers, for plagiarism. | www.bestessays.com<br>www.superiorpapers.com |
| Child Abuse Content | cprn | 1064 | Worldwide illegal child sexual abuse content. | — |

| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| Cloud and Data Centers | serv | 1118 | Platforms used to serve cloud infrastructure or data center hosting to support an organization's applications, services, or data processing. Due to the de-centralized nature of these domains and IP addresses, a more specific category cannot be applied based on content or ownership. | www.azurewebsites.net<br>www.s3.amazonaws.com |
| Computer Security | csec | 1065 | Offering security products and services for corporate and home users. | www.computersecurity.com<br>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<br>www.w3.org |
| Conventions, Conferences and Trade Shows | expo | 1110 | Seminars, trade shows, conventions and conferences themed around a particular industry, market, or common interest. May include information about acquiring tickets, registration, abstract or presentation proposal guidelines, workshops, sponsorship details, vendor or exhibitor information, and other marketing or promotional material. This category includes academic, professional, as well as pop-culture events, all of which tend to be a short-lived or annual event. | www.thesmallbusinessexpo.com<br>www.makerfaire.com |
| Cryptocurrency | cryp | 1111 | Online brokerages and websites that enable users to trade cryptocurrencies; information regarding cryptocurrencies including analysis, commentary, advice, performance indexes, and price charts. General information about cryptomining and mining businesses are included in this category but domains and IP addresses directly involved in mining activities are categorized as Cryptomining. | www.coinbase.com<br>www.coinsutra.com |

| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| Cryptomining | mine | 1112 | Hosts that are actively participating in a cryptocurrency mining pool. | www.give-me-coins.com<br>www.slushpool.com |
| Dating | date | 1055 | Dating, online personals, matrimonial agencies. | www.eharmony.com<br>www.match.com |
| Digital Postcards | card | 1082 | Enabling sending of digital postcards and e-cards. | www.hallmarkecards.com<br>www.bluemountain.com |
| Dining and Drinking | food | 1061 | Eating and drinking establishments; restaurants, bars, taverns, and pubs; restaurant guides and reviews. | www.zagat.com<br>www.experiencethepub.com |
| DIY Projects | diy | 1097 | Guidance and information to create, improve, modify, decorate and repair something without the aid of experts or professionals. | www.diy-tips.co.uk<br>www.thisoldhouse.com |
| DNS-Tuneling | tunn | 1122 | Sites that provide DNS Tunneling as a service. These services can be for PC or mobile and create a VPN connection specifically over DNS to send traffic that may bypass corporate policies and inspection. | |
| DoH and DoT | doht | 1113 | Encrypted DNS requests using either the DNS over HTTPS (DoH) protocol or the DNS over TLS protocol. These protocols are typically used as a layer of security and privacy by end-users, but the encryption hides the destination of the request and passes it through a third-party. | www.cloudflare-dns.com<br>www.dns.google.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 |
| Dynamic DNS Provider | ddns | 1114 | sers may use dynamic DNS services to make certain applications or content accessible via the web from endpoints hosted on dynamically assigned IP addresses. Access is granted through a hostname on the domain owned by the dynamic DNS service. | www.noip.com<br>www.afraid.org |

| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| 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<br>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<br>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<br>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 Medicine." | www.fashion.net<br>www.styleseat.com |
| File Transfer Services | fts | 1071 | File transfer services with the primary purpose of providing download services and hosted file sharing | www.sharefile.com<br>www.wetransfer.com |
| Filter Avoidance | filt | 1025 | Promoting and aiding undetectable and anonymous web usage, including cgi, php and glype anonymous proxy services. | www.bypassschoolfilter.com<br>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." | www.finance.yahoo.com<br>www.bankofamerica.com |

| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| Freeware and Shareware | free | 1068 | Providing downloads of free and shareware software. | www.freewarehome.com<br>www.filehippo.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 Medicine." Government-run lotteries are classified as "Lotteries". | www.888.com<br>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<br>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<br>www.law.com |
| Hacking | hack | 1050 | Discussing ways to bypass the security of websites, software, and computers. | www.hackthissite.org<br>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<br>www.aryanunity.com |

| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| Health and Medicine | hmed | 1104 | 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). | www.webmd.com<br>www.health.com |
| Humor | lol | 1079 | Jokes, sketches, comics and other humorous content. Adult humor likely to offend is classified as "Adult." | www.pun.me<br>www.jokes.com |
| Hunting | hunt | 1022 | Hunting and Fishing Professional or sport hunting; gun clubs and other hunting related sites. | www.bulletsafaris.com<br>www.mfha.org |
| 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<br>www.pyrobin.com |
| 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.keygenninja.com<br>www.rootscrack.com |
| Illegal Drugs | drug | 1047 | Information about recreational drugs, drug paraphernalia, drug purchase and manufacture. | www.shroomery.org<br>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<br>www.webstat.net |

| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| Internet of Things | iot | 1116 | Domains used to monitor the general health, activity, or aid in the configuration of Internet of Things (IoT) and other network-aware electronics. Additionally these sites may provide software or firmware updates or allow remote access to administer the device. IoT exists in both consumer and professional segments, in products such as printers, televisions, thermostats, system monitoring, automation, and smart appliances. | www.samsungotn.net<br>www.transport.nest.com |
| Internet Telephony | voip | 1067 | Telephonic services using the Internet. | www.skype.com<br>www.getvoca.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<br>www.monster.com |
| Lingerie and Swimsuits | ling | 1031 | Intimate apparel and swimwear, especially when modeled. | www.swimsuits.com<br>www.victoriassecret.com |
| Lotteries | lotr | 1034 | Sweepstakes, contests and state-sponsored lotteries. | www.calottery.com<br>www.flalottery.com |
| Military | mil | 1099 | Military, such as the armed forces; military bases; military organizations; anti-terrorism. | www.goarmy.com<br>www.todaysmilitary.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.cbfsms.com<br>www.zedge.net |
| Museums | muse | 1117 | Museums and exhibits, both online and physical, dedicated to preserving information regarding subjects that could be of general interest or highly specialized. Subjects could range from art, history, science, or be of cultural importance. | www.ushmm.org<br>www.[illegible] |

| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| Nature and Conservation | ncon | 1106 | Sites related to 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). | www.nature.org<br>www.thepottedgarden.co.uk |
| News | news | 1058 | News; headlines; newspapers; television stations; magazines; weather; ski conditions. | www.cnn.com<br>www.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<br>www.unions.org |
| Non-sexual Nudity | nsn | 1060 | Nudism and nudity; naturism; nudist camps; artistic nudes. | www.1001fessesproject.com<br>www.naturistsociety.com |
| Not Actionable | nact | 1103 | Sites that have been inspected but are unreachable or do not have enough content to be assigned a category. | — |
| Online Communities | comm | 1024 | Affinity groups; special interest groups; web newsgroups; message boards. Excludes websites classified as “Professional Networking” or “Social Networking.” | www.reddit.com<br>www.stackexchange.com |
| Online Document Sharing and Collaboration | docs | 1115 | Cloud-based software used to create, convert, or edit documents. Collaboration and sharing features may be available with access permissions typically configured by the author. Documents may be stored online or available to download. | www.pastebin.com<br>www.docs.google.com |

| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| Online Meetings | meet | 1100 | Online meetings; desktop sharing; remote access and other tools that facilitate multi-location collaboration | www.join.me<br>www.teamviewer.com |
| Online Storage and Backup | osb | 1066 | Offsite and peer-to-peer storage for backup, sharing, and hosting. | www.adrive.com<br>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<br>www.etrade.com |
| Organizational Email | pem | 1085 | Websites used to access business email (often via Outlook Web Access). | www.mail.zoho.com<br>www.webmail.edmc.edu |
| Paranormal | prnm | 1101 | UFOs; ghosts; cryptid; telekenesis; urban legends; and myths. | www.ghoststudy.com<br>www.ufocasebook.com |
| 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<br>www.cricketbuzz.com |
| Peer File Transfer | p2p | 1056 | Peer-to-peer file request websites. This does not track the file transfers themselves. | www.bittorrent.com<br>www.torrentdownloads.me |
| Personal Sites | pers | 1081 | Websites about and from private individuals; personal homepage servers; websites with personal contents; personal blogs with no particular theme. | www.blogmaverick.com<br>www.stallman.org |
| Personal VPN | pvpn | 1102 | Virtual private network (VPN) sites or tools that are typically for personal use, and, may or may not be approved for corporate usage. | www.openvpn.net<br>www.torvpn.com |
| Photo Search and Images | img | 1090 | Facilitating the storing and searching for, images, photographs, and clip-art. | www.flickr.com<br>www.photobucket.com |

| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| Politics | pol | 1083 | Websites of politicians; political parties; news and information on politics, elections, democracy, and voting. | www.politics.com<br>www.gp.org |
| 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<br>www.youporn.com |
| Private IP Addresses as Host | piah | 1121 | Private IP addresses which are used as the host part of a URL. Private IP addresses are meant for internal use behind border routers only, so they are not publicly routable. | |
| Professional Networking | pnet | 1089 | Social networking for the purpose of career or professional development. See also “Social Networking.” | www.linkedin.com<br>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<br>www.zillow.com |
| Recipes and Food | reci | 1105 | Sites dedicated to sharing or discussing information about cooking, recipes, and food or non-alcoholic beverages; cultural aspects of cuisine and food; diet descriptions and adherence tips, general nutrition information about foods. Use and instruction on cooking appliances and utensils. Food celebrity, lifestyle, and enthusiast blogs. | www.allrecipes.com<br>www.seriouseats.com |
| Reference | ref | 1017 | City and state guides; maps, time; reference sources; dictionaries; libraries. | www.wikipedia.org<br>www.yellowpages.com |
| Regional Restricted Sites (Germany) | xdeu | 1125 | URLs that are restricted in Germany due to content which may be unlawful as determined by the regional government. | |
| Regional Restricted Sites (Great Britain) | xgbr | 1123 | URLs that are restricted in Great Britain due to content which may be unlawful as determined by the regional government. | |

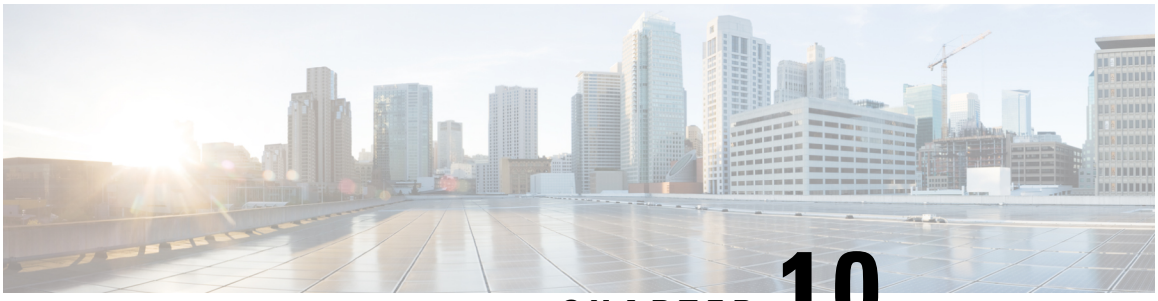
| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| Regional Restricted Sites (Italy) | xita | 1124 | URLs that are restricted in Italy due to content which may be unlawful as determined by the regional government. | |
| Regional Restricted Sites (Poland) | xpol | 1126 | URLs that are restricted in Poland due to content which may be unlawful as determined by the regional government. | www.betsafe62.com<br>www.tornadobet69.com |
| Religion | rel | 1086 | Religious content, information about religions; religious communities. | www.religionfacts.com<br>www.religioustolerance.org |
| SaaS and B2B | saas | 1080 | Web portals for online business services; online meetings. | www.netsuite.com<br>www.salesforce.com |
| Safe for Kids | kids | 1057 | Directed at, and specifically approved for, young children. | www.discoverykids.com<br>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<br>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<br>www.google.com |
| Sex Education | sxed | 1052 | Factual websites dealing with sex; sexual health; contraception; pregnancy. | www.avert.org<br>www.scarleteen.com |
| Shopping | shop | 1005 | Bartering; online purchasing; coupons and free offers; general office supplies; online catalogs; online malls. | www.amazon.com<br>www.shopping.com |
| Social Networking | snet | 1069 | Social networking. See also "Professional Networking." | www.facebook.com<br>www.twitter.com |
| 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<br>www.anthropology.net |
| Society and Culture | scty | 1010 | Family and relationships; ethnicity; social organizations; genealogy; seniors; child-care. | www.childcareaware.org<br>www.familysearch.org |

| URL Category | Abbreviation | Code | Description | Example URLs |
|---|---|---|---|---|
| Software Updates | swup | 1053 | Websites that host updates for software packages. | www.softwarepatch.com<br>www.windowsupdate.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<br>www.recreation.gov |
| Streaming Audio | aud | 1073 | Real-time streaming audio content including Internet radio and audio feeds. | www.live-radio.net<br>www.shoutcast.com |
| Streaming Video | vid | 1072 | Real-time streaming video including Internet television, web casts, and video sharing. | www.hulu.com<br>www.youtube.com |
| Terrorism and Violent Extremism | terr | 1119 | Terrorist or extremist websites that promote death or violence as part of their ideology. Sites may contain graphic or disturbing images, videos, and text. Some sites may not advocate terrorism but share first-hand material of a violent nature. | |
| 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 Medicine.” | www.bat.com<br>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<br>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<br>www.lonelyplanet.com |
| URL Shorteners | shrt | 1120 | Domains used to shorten long URLs, brand URLs, or may obscure the final destination of a hyperlink. | www.bit.ly<br>www.tinyurl.com |

| URL Category | Abbreviation | Code | Description | Example 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<br>www.gunbroker.com |
| Web Cache and Archives | cach | 1108 | Cached or archived web content often stored for preservation or to decrease load times. | www.archive.org<br>www.webcache.googleusercontent.com |
| Web Hosting | whst | 1037 | Website hosting; bandwidth services. | www.bluehost.com<br>www.godaddy.com |
| Web Page Translation | tran | 1063 | Translation of web pages between languages. | www.babelfish.com<br>www.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." | www.mail.yahoo.com<br>www.outlook.com |

### Related Topics

- Managing Updates to the Set of URL Categories , on page 168
- Reporting Uncategorized and Misclassified URLs, on page 167



CHAPTER 10

# Create Policies to Control Internet Requests

This topic contains the following sections:


- Overview of Policies: Control Intercepted Internet Requests, on page 213
- Managing Web Requests Through Policies Task Overview, on page 215
- Managing Web Requests Through Policies Best Practices, on page 215
- Policies, on page 215
- Policy Configuration, on page 225
- Block, Allow, or Redirect Transaction Requests, on page 230
- Client Applications, on page 231
- Time Ranges and Quotas, on page 233
- Access Control by URL Category, on page 236
- Remote Users, on page 238
- Troubleshooting Policies, on page 240


# 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.

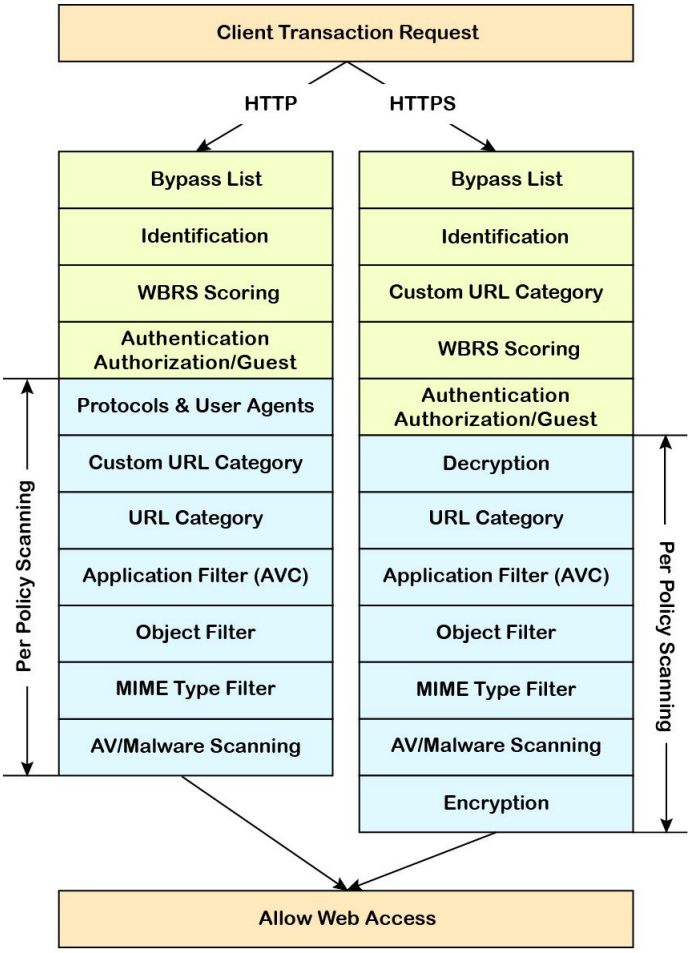
The Web Security Appliance uses multiple policy types to manage different aspects of web requests. Policy types might fully manage transactions by themselves or pass transactions along to other policy types for additional processing. Policy types can be groups by the functions they perform, such as access,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

# Intercepted HTTP/HTTPS Request Processing

The following diagram depicts the flow of an intercepted Web request as it is processed by the appliance.

***Figure 3: HTTP/HTTPS Transaction Flow***




Also see the following diagrams depicting various transaction processing flows:

- Figure 1: Identification Profiles and Authentication Processing – No Surrogates and IP-based Surrogates, on page 137
- Figure 2: Identification Profiles and Authentication Processing – Cookie-based Surrogates, on page 138
- Figure 4: Policy Group Transaction Flow for Access Policies, on page 219
- Figure 7: Policy Group Transaction Flow for Decryption Policies, on page 245
- Controlling HTTPS Traffic, on page 247

# 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, on page 99 |
| 2 | (For upstream proxies) Create a proxy group. | Creating Proxy Groups for Upstream Proxies, on page 22 |
| 2 | (Optional) Create Custom Client Applications | Client Applications, on page 231 |
| 3 | (Optional) Create Custom URL Categories | Creating and Editing Custom URL Categories, on page 183 |
| 4 | Create Identification Profiles | Classifying Users and Client Software, on page 131 |
| 5 | (Optional) Create time ranges to Limit Access by Time of Day | Time Ranges and Quotas, on page 233 |
| 6 | Create and Order Policies | • Creating a Policy , on page 219<br>• Policy Order, on page 218 |

# 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 do not contain the primary group.

# Policies

- Policy Types, on page 215
- Policy Order, on page 218
- Creating a Policy , on page 219

## Policy Types

| Policy Type | Request Type | Description | Link to task |
|---|---|---|---|
| Access | • HTTP<br>• Decrypted HTTPS<br>• FTP | Block, allow or redirect inbound HTTP, FTP, and decrypted HTTPS traffic.<br>Access policies also manage inbound encrypted HTTPS traffic if the HTTPS proxy is disabled. | Creating a Policy , on page 219 |

| Policy Type | Request Type | Description | Link to task |
|---|---|---|---|
| SOCKS | • SOCKS | Allow or block SOCKS communication requests. | Creating a Policy , on page 219 |
| Application Authentication | • application | Allow or deny access to a Software as a Service (SaaS) application.<br>Use single sign-on to authenticate users and increase security by allowing access to applications to be quickly disabled.<br>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. | Creating SaaS Application Authentication Policies, on page 144 |
| Encrypted HTTPS Management | • HTTPS | Decrypt, pass through, or drop HTTPS connections.<br>AsyncOS passes decrypted traffic to Access policies for further processing. | Creating a Policy , on page 219 |
| Data Security | • HTTP<br>• Decrypted HTTPS<br>• 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 , on page 219 |
| External DLP (Data Loss Prevention) | • HTTP<br>• Decrypted HTTPS<br>• 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 , on page 219 |

| Policy Type | Request Type | Description | Link to task |
|---|---|---|---|
| Outbound Malware Scanning | • HTTP<br>• Decrypted HTTPS<br>• FTP | Block, monitor, or allow requests to upload data that may contain malicious data.<br>Prevent malware that is already present on your network from being transmitted to external networks. | Creating a Policy , on page 219 |
| Routing | • HTTP<br>• HTTPS<br>• FTP | 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.<br>If multiple upstream proxies are available, the Web Security Appliance can use load balancing techniques to distribute data to them.<br>Retian the client's source IP address, change it to the web proxy IP, or a custom IP using IP Spooing profile. | Creating a Policy , on page 219 |

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 user-request types they manage, and the actions they perform on those requests. Each policy definition has two main sections:

- **Identification Profiles and Users** – Identification Profiles 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.
- **Advanced** – The criteria used to identify users 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.
  - **Protocols** – Allow the transfer of data between various networking devices such as http, https, ftp, etc.
  - **Proxy Ports** – the numbered port by which the request accesses the web proxy,
  - **Subnets** – The logical grouping of connected network devices (such as geographic location or Local Area Network [LAN]), where the request originated
  - **Time Range** – 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 updaters and Web browsers) 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 user agents but cannot re-use these definitions other policies.



**Note** When you define multiple membership criteria, the client request must meet all criteria to match the policy.

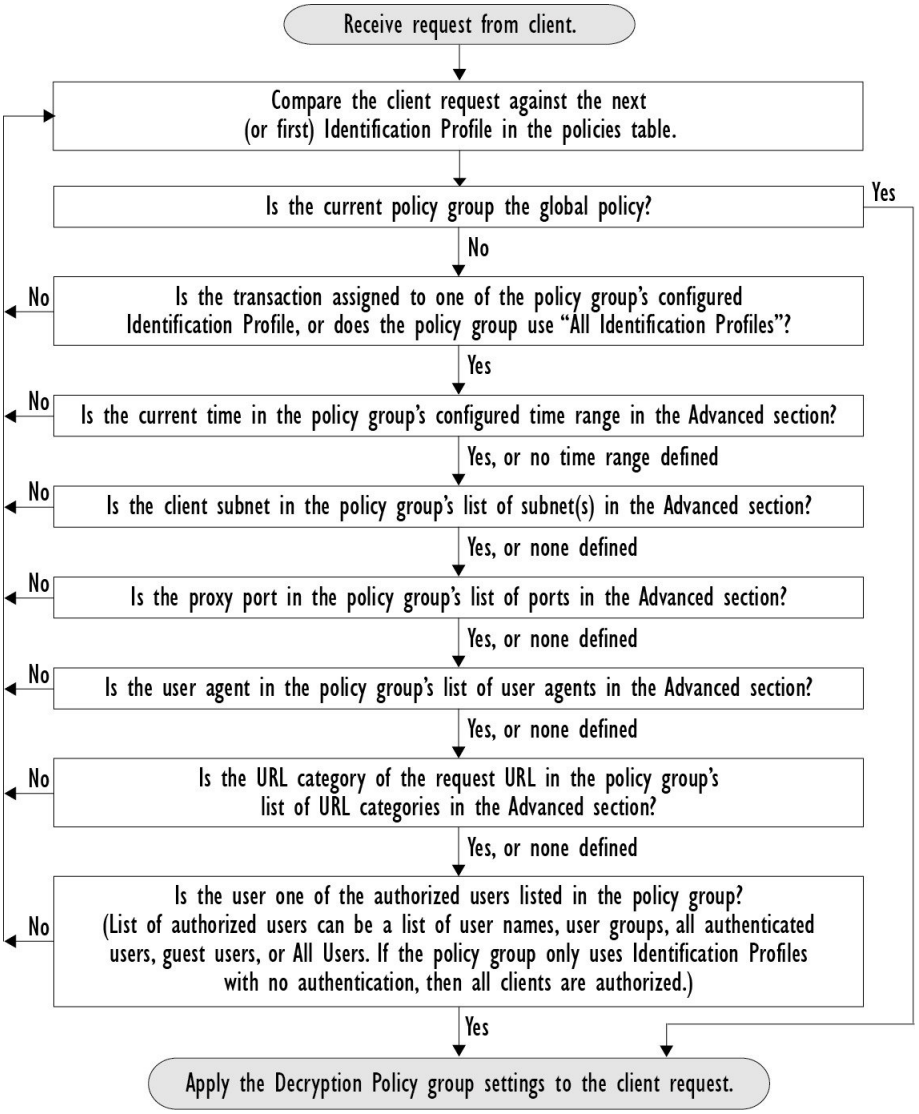
# Policy Order

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 re-ordered.

The following diagram depicts the flow of a client request through the Access policies table.

*Figure 4: Policy Group Transaction Flow for Access Policies*




# Creating a Policy

### Before you begin

- Enable the appropriate proxy:
  - Web Proxy (for HTTP, decrypted HTTPS, and FTP)
  - HTTPS Proxy
  - SOCKS Proxy
- Create associated Identification Profiles.

- Understand Policy Order, on page 218.
- (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. See Time Ranges and Quotas, on page 233.
- (Optional) Create associated URL categories. See Creating and Editing Custom URL Categories, on page 183.

### Procedure

**Step 1** In the **Policy Settings** section, use the **Enable Identity** check box to enable this policy, or to quickly disable it without deleting it.

**Step 2** Assign a unique policy **Name**.

**Step 3** A **Description** is optional.

**Step 4** From the Insert Above drop-down list, choose where this policy is to appear in the table.

**Note**
Arrange policies such that, from top to bottom of the table, they are in most-restrictive to least-restrictive order. See Policy Order, on page 218 for more information.

**Step 5** In the **Policy Expires** area, check the **Set Expiration for Policy** check box to set the expiry time for the policy. Enter the date and time for the policy expiration that you want to set. The policies are automatically disabled once they exceed the set expiry time.

**Note**
System checks the policies every minute to disable the policies which get expired during the minute. For example, if a policy is set to expire at 11:00, at maximum it will be disabled by 11:01.

Policy Expiry feature is applicable only for Access, Decryption, and Web Traffic Tap policies.

You will receive an email prior to three days of the policy expiry and another one upon policy expiry.

**Note**
To receive alerts, you must enable Policy Expiration alerts using **System Administration** > **Alerts** . See Policy Expiration Alerts, on page 528

You can set the policy expiration time through Cisco Content Security Management Appliances as well. The policies will get expired after the set expiry time but will not be shown as disabled in the Cisco Content Security Management Appliances GUI.

Once you set the policy expiration feature, the expiry happens based on the appliance's local time settings.

**Step 6** In the **Policy Member Definition** section, specify how user and group membership is defined: from the Identification Profiles and Users list, choose one of the following:

- **All Identification Profiles** – This policy will apply to all existing profiles. You must also define at least one **Advanced** option.
- **Select One or More Identification Profiles** – A table for specifying individual Identification Profiles appears, one profile-membership definition per row.

**Step 7** If you chose **All Identification Profile**s:

a) Specify the authorized users and groups to which this policy applies by selecting one of the following options:

- **All Authenticated Users** – All users identified through authentication or transparent identification.
- **Selected Groups and Users** – Specified users and groups are used.

  To add or edit the specified **ISE Secure Group Tags** (SGTs) and the specified Users, click the link following the appropriate label. For example, click the list of currently specified users to edit that list. See Adding and Editing Secure Group Tags for a Policy, on page 223 for more information.

  If you use ISE, you can add or edit ISE Secure Group Tags. This is not supported in ISE-PIC deployments. To add or edit the specified **ISE Groups**, click the link following the label. This option is specific to ISE-PIC.
- **Guests** – Users connected as guests and those failing authentication.
- **All Users** – All clients, whether authenticated or not. If this option is selected, at least one **Advanced** option also must be provided.

**Step 8** If you chose **Select One or More Identification Profiles**, a profile-selection table appears.

a) Choose an Identification Profile from the Select Identification Profile drop-down list in the Identification Profiles column.

b) Specify the Authorized Users and Groups to which this policy applies:

- **All Authenticated Users** – All users identified through authentication or transparent identification.
- **Selected Groups and Users** – Specified users and groups are used.

  To add or edit the specified ISE Secure Group Tags (SGTs) and the specified Users, click the link following the appropriate label. For example, click the list of currently specified users to edit that list. See Adding and Editing Secure Group Tags for a Policy, on page 223 for more information.
- **Guests** – Users connected as guests and those failing authentication.

c) To add a row to the profile-selection table, click **Add Identification Profile**. To delete a row, click the trash-can icon in that row.

Repeat steps (a) through (c) as necessary to add all desired Identification Profiles.

**Step 9** Expand the **Advanced** section to define additional group membership criteria. (This step may be optional depending on selection in the **Policy Member Definition** section. Also, some of the following options will not be available, depending on the type of policy you are configuring.) .

| Advanced Option | Description |
|---|---|
| Protocols | Select the protocols to which this policy will apply. **All others** means any protocol not selected. If the associated identification profile applies to specific protocols, this policy applies to those same protocols |

| Advanced Option | Description |
|---|---|
| Proxy Ports | Applies this policy only to traffic using specific ports to access the web proxy. Enter one or more port numbers, separating multiple ports with commas.<br>For explicit forward connections, this is the port configured in the browser.<br>For transparent connections, this is the same as the destination port.<br>**Note**<br>If the associated identification profile applies only to specific proxy ports, you cannot enter proxy ports here. |
| Subnets | Applies this policy only to traffic on specific subnets. Select **Specify subnets** and enter the specific subnets, separated by commas.<br>Leave **Use subnets from selected Identities** selected if you do not want additional filtering by subnet.<br>**Note**<br>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. |
| Time Range | You can apply time ranges for policy membership:<br>• Time Range – Choose a previously defined time range (Time Ranges and Quotas, on page 233).<br>• Match Time Range – Use this option to indicate whether this time range is inclusive or exclusive. In other words, whether to match only during the range specified, or at all times except those in the specified range. |
| URL Categories | You can restrict policy membership by specific destinations (URLs) and by categories of URLs. Select all desired custom and predefined categories. See Creating and Editing Custom URL Categories, on page 183 for information about custom categories. |
| User Agents | You can select specific user agents, and define custom agents using regular expressions, as part of membership definition for this policy.<br>• **Common User Agents**<br>  • **Browsers** – Expand this section to select various Web browsers.<br>  • **Others** – Expand this section to select specific non-browser agents such as application updaters.<br>• **Custom User Agents** – You can enter one or more regular expressions, one per line, to define custom user agents.<br>• **Match User Agents** – Use this option to indicate whether these user-agent specifications are inclusive or exclusive. In other words, whether membership definition includes only the selected user agents, or specifically excludes the selected user agents. |

## Adding and Editing Secure Group Tags for a Policy

To change the list of Secure Group Tags (SGTs) assigned to a particular Identification Profile in a policy, click the link following the ISE Secure Group Tags label in the Selected Groups and Users list on the Add/Edit Policy page. (See Creating a Policy , on page 219.) This link is either "No tags entered," or it is a list of currently assigned tags. The link opens the Add/Edit Secure Group Tags page.

All SGTs currently assigned to this policy are listed in the Authorized Secure Group Tags section. All SGTs available from the connected ISE server are listed in the Secure Group Tag Search section.

### Procedure

**Step 1** To add one or more SGTs to the Authorized Secure Group Tags list, select the desired entries in the Secure Group Tag Search section, and then click **Add**.

**Note**

- The SGTs already added, are highlighted in green. To quickly find a specific SGT in the list of those available, enter a text string in the **Search** field.
- When a Web Security Appliance is connected to ISE/ISE-PIC, default SGTs from ISE/ISE-PIC are also displayed. These SGTs will not have users assigned. Ensure that you select the correct SGTs.

**Step 2** To remove one or more SGTs from the Authorized Secure Group Tags list, select those entries and then click **Delete**.

**Step 3** Click Done to return to the Add/Edit Group page.

### What to do next

**Related Topics**

- Time Ranges and Quotas, on page 233
- Using Client Applications in Policies, on page 232

## Adding Routing Destination and IP Spoofing Profile to Routing Policy

You can configure how the web proxy forwards the web traffic and the requests the source IP address by configuring the routing destination and IP spoofing profile in routing policies.



**Note**

- The global routing policy is enabled by default even if an upstream proxy group is not configured on the appliance.
- IP spoofing profiles are not related to routing destination, and can be configured independently.
- Routing Policy can be enabled without configuring an upstream proxy.

**Note** To configure an upstream proxy group for a routing policy in Security Management appliance, save the configuration file of the Web Security Appliance and import it on the Security Management appliance. Otherwise, the Security Management appliance shows the upstream proxy as "Not Found" and the routing policy will be disabled after the config push.

### Procedure

**Step 1** Choose **Web Security Manager** > **Routing Policies**.

**Step 2** On the **Routing Policies** page, click the link under **Routing Destination** column for the routing policy that you want to configure the upstream proxy group.

**Step 3** Choose an appropriate upstream proxy group for the selected policy from the following:

| Action | Description |
|---|---|
| Use Global Policy Settings | The web proxy uses the settings defined in the Global Policy. This is the default action for user defined policy groups. By default, the routing destination for Global Routing Policy is set as **Direct Connection**.<br>Applies to user defined policy groups only. |
| Direct Connection | The web proxy forwards web traffic directly to its destination web server. |
| Custom upstream proxy group | The web proxy redirects the web traffic to an external upstream proxy group. For more information about creating upstream proxy groups, see Upstream Proxies, on page 22. |

**Step 4** On the **Routing Policies** page, click the link under **IP Spoofing** column for the routing policy that you want to configure the IP spofing profile.

**Step 5** Choose an appropriate IP spoofing profile for the selected policy from the following:

| Action | Description |
|---|---|
| Use Global Policy Settings | The web proxy uses the settings defined in the Global Policy. This is the default action for user defined policy groups. By default, the IP spoofing is disabled for the Global Routing Policy.<br>Applies to user defined policy groups only. |
| Do No Use IP Spoofing | The web proxy changes the request source IP address to match its own address to increase security. |
| Use Client IP | The web proxy retains the source address so that it appears to originate from the source client rather than from the Web Security Appliance . |
| Custom spoofing profile name | The web proxy changes the request source IP address to custom IP defined in the selected custom IP spoofing profile name. |

**Step 6** **Submit** and **Commit** your changes.

### What to do next

### Related Topics

- Upstream Proxies, on page 22
- Web Proxy IP Spoofing, on page 70

# Policy Configuration

Each row in a table of policies represents a policy definition, and each column displays current contains a link to a configuration page for that element of the policy.

**Note** Of the following policy-configuration components, you can specify the "Warn" option only with URL Filtering.

| Option | Description |
|---|---|
| Protocols and User Agents | 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 Filtering | 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 block, monitor, warn, or set quota-based or time-based filters.<br>You can also create custom URL categories and then choose to block, redirect, allow, monitor, warn, or apply quota-based or time-based filters for Websites in the custom categories. See Creating and Editing Custom URL Categories, on page 183 for information about creating custom URL categories.<br>In addition, you can add exceptions to blocking of embedded or referred content. |
| 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 Types, and by individual applications. You can also apply controls to particular application behaviors, such as file transfers, within a particular application. See Managing Access to Web Applications, on page 303 for configuration information. |
| Objects | These options let you configure the Web Proxy to block file downloads based on file characteristics, such as file size, file type, and MIME type. An object is, generally, any item that can be individually selected, uploaded, downloaded and manipulated. See Access Policies: Blocking Objects, on page 226 for information about specifying blocked objects. |

| Option | Description |
|---|---|
| Anti-Malware and Reputation | 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.<br><br>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.<br><br>For more information, see Anti-Malware and Reputation Settings in Access Policies, on page 272 and Configuring File Reputation and Analysis Features, on page 285. |
| Delete | Deletes the created policy. |

# Access Policies: Blocking Objects

You can use the options on the Access Policies: Objects page to block file downloads based on file characteristics, such as file size, file type, and MIME type. An object is, generally, any item that can be individually selected, uploaded, downloaded and manipulated.

You can specify a number of types of objects to be blocked by each individual Access policy, and by the Global policy. These object types include Archives, Document Types, Executable Code, Web Page Content, and so on.

### Procedure

**Step 1** On the Access Policies page (**Web Security Manager** > **Access Policies**), click the link in the **Objects** column of the row representing the policy you wish to edit.

**Step 2** Choose the desired type of object blocking for this Access policy:

- **Use Global Policy Objects Blocking Settings** – This policy uses the object-blocking settings defined for the Global Policy; these settings are displayed in read-only mode. Edit the settings for the Global Policy to change them.
- **Define Custom Objects Blocking Settings** – You can edit all object-blocking settings for this policy.
- **Disable Object Blocking for this Policy** – Object blocking is disabled for this policy; no object-blocking options are presented.

**Step 3** If you chose **Define Custom Objects Blocking Settings** in the previous step, select and deselect object-blocking options on the Access Policies: Objects page as needed.

| | |
|---|---|
| **Object Size** | You can block objects based on their download size:<br>• **HTTP/HTTPS Max Download Size** – Either provide the maximum object size for HTTP/HTTPS download (objects larger than this will be blocked), or indicate that there is no maximum size for object download via HTTP/HTTPS.<br>• **FTP Max Download Size** – Either provide the maximum object size for FTP download (objects larger than this will be blocked), or indicate that there is no maximum size for object download via FTP. |
| **Block Object Type** | |
| **Archives** | Expand this section to select types of Archive files that are to be blocked. This list includes Archive types such as ARC, BinHex, and StuffIt. |

| | |
|---|---|
| **Inspectable Archives** | Expand this section to select whether to **Allow**, **Block**, or **Inspect** specific types of Inspectable Archive files. Inspectable Archives are archive or compressed files that the Web Security Appliance can inflate to inspect each of the contained files in order to apply the file-type block policy. The Inspectable Archives list includes archive types such as 7zip, Microsoft CAB, RAR, and TAR.<br><br>The following points apply to archive inspection:<br>• Only archive types marked **Inspect** will be inflated and inspected.<br>• Only one archive will be inspected at a time, Additional concurrent inspectable archives may not be inspected.<br>• If an inspected archive contains a file type that is assigned the Block action by the current policy, the entire archive will be blocked, regardless of any allowed file types it may contain.<br>• An inspected archive that contains an unsupported archive type will be marked as "unscannable." If it contains a blocked archive type, it will be blocked.<br>• Password-protected and encrypted archives are not supported and will be marked as "unscannable."<br>• An inspectable archive which is incomplete or corrupt is marked as "unscannable."<br>• The **DVS Engine Object Scanning Limits** value specified for the **Anti-Malware and Reputation** global settings also applies to the size of an inspectable archive; an object exceeding this size is marked as "unscannable." See Enabling Anti-Malware and Reputation Filters, on page 269 for information about this object size limit.<br>• An inspectable archive marked as "unscannable" can be either Blocked in its entirety or Allowed in its entirety.<br>• When access policies are configured to block custom MIME types, and archive inspection is enabled:<br>  • If the appliance directly downloads a file with the custom MIME type as part of the content-type header, access is blocked.<br>  • If the same file is part of a ZIP/archive file, the appliance inspects the archive and determines the MIME type based on its own MIME evaluation. If the MIME evaluated by the appliance's engine does not match the configured custom MIME type, the content is not blocked.<br>• The appliance can inspect configured archives but it has the limitation to inspect certain archives such as RAR and 7-Zip.<br><br>See Archive Inspection Settings, on page 229 for information about configuring archive inspection. |
| **Document Types** | Expand this section to select types of text documents to be blocked. This list includes document types such as FrameMaker, Microsoft Office, and PDF. |
| **Executable Code** | Expand this section to select types of executable code to be blocked. The list includes Java Applet, UNIX Executable and Windows Executable. |

| | |
|---|---|
| **Installers** | Types of installers to be blocked; the list includes UNIX/LINUX Packages. |
| **Media** | Types of media files to be blocked. The list includes Audio, Video and Photographic Image Processing Formats (TIFF/PSD). |
| **P2P Metafiles** | This list includes BitTorrent Links (`.torrent`). |
| **Web Page Content** | This list includes Flash and Images. |
| **Miscellaneous** | This list includes Calendar Data. |
| **Custom MIME Types** | You can define additional objects/files to be blocked based on MIME type.<br>Enter one or more MIME types in the **Block Custom MIME Types** field, one per line. |

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

## Archive Inspection Settings

You can Allow, Block, or Inspect specific types of Inspectable Archives for individual Access policies. Inspectable Archives are archive or compressed files that the Web Security Appliance can inflate to inspect each of the contained files in order to apply the file-type block policy. See Access Policies: Blocking Objects, on page 226 for more information about configuring archive inspection for individual Access policies.

**Note** During archive inspection, nested objects are written to disk for examination. The amount of disk space that can be occupied at any given time during file inspection is 1 GB. Any archive file exceeding this maximum disk-use size will be marked unscannable.

The Web Security Appliance 's Acceptable Use Controls page provides system-wide Inspectable Archives Settings; that is, these settings apply to archive extraction and inspection whenever enabled in an Access policy.

### Procedure

**Step 1** Choose **Security Services** > **Acceptable Use Controls**.

**Step 2** Click the **Edit Archives Settings** button.

**Step 3** Edit the Inspectable Archives Settings as needed.

- **Maximum Encapsulated Archive Extractions** – Maximum number of "encapsulated" archives to be extracted and inspected. That is, maximum depth to inspect an archive containing other inspectable archives. An encapsulated archive is one that is contained in another archive file. This value can be zero through five; depth count begins at one with the first nested file.

  The external archive is considered file zero. If the archive has files nested beyond this maximum nested value, the archive is marked as unscannable. Note that this will impact performance.

- **Block Uninspectable Archives** – If checked, the Web Security Appliance will block archives it failed to inflate and inspect.

**Step 4** **Submit** and **Commit Changes**.

# 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, on page 191.

**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.

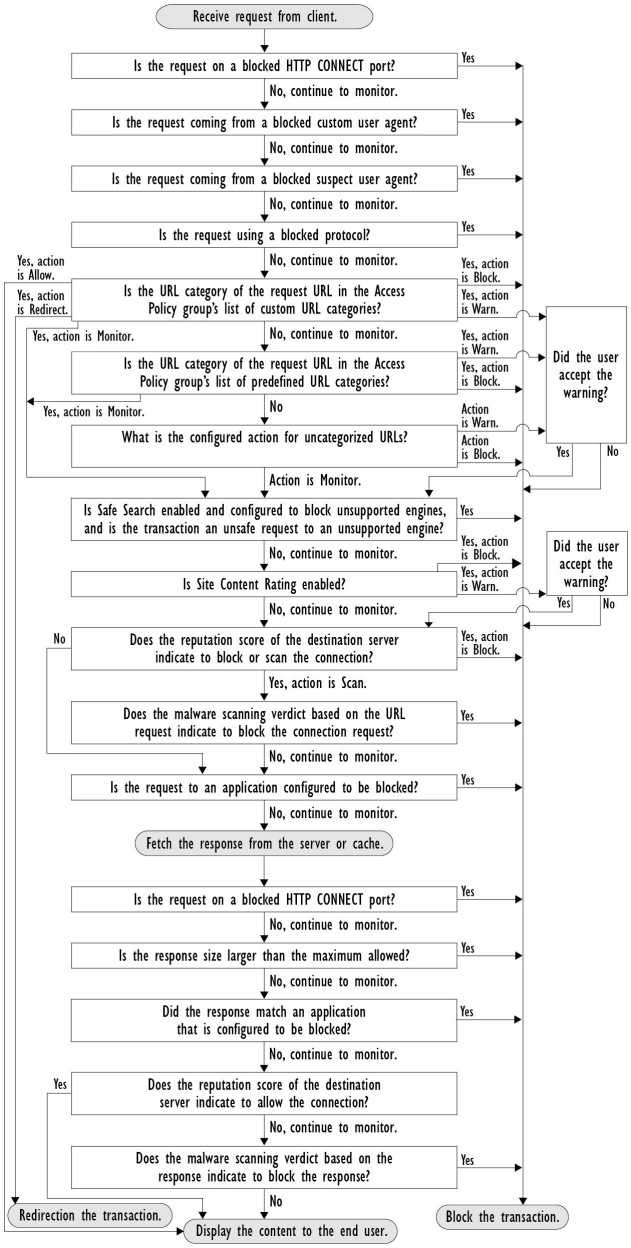
Generally, different types of policies control traffic based on the transport protocol.

| 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.

The following diagram shows how the Web Proxy determines which action to take on a request after it has assigned a particular Access Policy to the request. The Web reputation score of the destination server is evaluated only once, but the result is applied at two different points in the decision flow.

*Figure 5: Applying Access Policy Actions*




# 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

### Procedure

**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:

| Option | Method |
|---|---|
| Choose a predefined client application | Expand the Browser and Other sections and check the required client application check boxes.<br>**Tip**<br>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.<br>**Tip**<br>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

### Procedure

**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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Create an Identification Profile that does not require authentication. | Classifying Users and Client Software, on page 131 |
| **Step 2** | Set the Identification Profile membership as the client application to exempt. | Using Client Applications in Policies, on page 232 |
| **Step 3** | Place the Identification Profile above all other Identification Profiles in the policies table that require authentication. | Policy Order, on page 218 |

# Time Ranges and Quotas

You can apply time ranges and time and volume quotas to access policies and decryption policies to restrict when a user has access, as well as their maximum connection time or data volume (also referred to as a "bandwidth quota").

- Time Ranges for Policies and Acceptable Use Controls, on page 233
- Time and Volume Quotas, on page 234

## Time Ranges for Policies and Acceptable Use Controls

Time ranges are defined periods of time during which policies and acceptable use controls apply.

**Note** You cannot use time ranges to define the times at which users must authenticate. Authentication requirements are defined in Identification Profiles, which do not support time ranges.

- Creating a Time Range, on page 233

### Creating a Time Range

### Procedure

**Step 1** Choose **Web Security Manager** > **Define Time Ranges and Quotas**.

**Step 2** Click **Add Time Range**.

**Step 3** Enter a name for the time range.

**Step 4** Choose a **Time Zone** option:

- Use **Time Zone Setting From Appliance** – Use the same time zone as the Web Security Appliance .
- **Specify Time Zone for this Time Range** – Define a different time zone, either as a GMT Offset, or as a region, country and a specific time zone in that country.

**Step 5** Check one or more **Day of Week** check boxes.

**Step 6** Select a **Time of Day** option:

- **All Day** – Use the full 24-hour period.
- **From** and **To** – Define a specific range of hours: enter a start time and end time in HH:MM (24-hour format).

**Tip**
Each time range defines a start time and an end-time boundary. 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** Submit and commit your changes.

# Time and Volume Quotas

Quotas allow individual users to continue accessing an Internet resource (or a class of Internet resources) until they exhaust the data volume or time limit imposed. AsyncOS enforces defined quotas on HTTP, HTTPS and FTP traffic.

As a user approaches either their time or volume quota, AsyncOS displays first a warning, and then a block page.

Please note the following regarding use of time and volume quotas:

- If AsyncOS is deployed in transparent mode and HTTPS proxy is disabled, there is no listening on port 443, and requests are dropped. This is standard behavior. If AsyncOS is deployed in explicit mode, you can set quotas in your access policies.

  When HTTPS proxy is enabled, possible actions on a request are pass-through, decrypt, drop, or monitor. Overall, quotas in decryption policies are applicable only to the pass-through categories.

  With pass-through, you will also have the option to set quotas for tunnel traffic. With decrypt, this option is not available, as the quotas configured in the access policy will be applied to decrypted traffic.

- If URL Filtering is disabled or if its feature key is unavailable, AsyncOS cannot identify the category of a URL, and the **Access Policy** > **URL Filtering** page is disabled. Thus, the feature key needs to be present, and Acceptable Use Policies enabled, to configure quotas..
- Many websites such as Facebook and Gmail auto-update at frequent intervals. If such a website is left open in an unused browser window or tab, it will continue to consume the user's quota of time and volume.
- When you restart the proxy and the high-performance mode is:
  - **Enabled** - Time and volume quotas are not reset. Quotas are automatically reset once within the 24-hour window based on the configured time.
  - **Disabled** - Time and volume quotas are reset. The reset impact remains only for the current 24-hour window as the quotas are automatically reset once within 24 hours. Proxy may restart due to configuration changes or proxy process crash.

- Your EUN pages (both warning and block) cannot be displayed for HTTPS even when decrypt-for-EUN option is enabled.

**Note** The most restrictive quota will always apply when more than one quota applies to any given user.


- Volume Quota Calculations, on page 235
- Time Quota Calculations, on page 235
- Defining Time and Volume Quotas, on page 235


## Volume Quota Calculations

Calculation of volume quotas is as follows:

- HTTP and decrypted HTTPS traffic – The HTTP request and response body are counted toward quota limits. The request headers and response headers will not be counted toward the limits.
- Tunnel traffic (including tunneled HTTPS) – AsyncOS simply shuttles the tunneled traffic from the client to the server, and vice versa. The entire data volume of the tunnel traffic is counted toward quota limits.
- FTP – The control-connection traffic is not counted. The size of the file uploaded and downloaded is counted toward quota limits.

**Note** Only client-side traffic is counted toward quota limits. Cached content also counts toward the limit, as client-side traffic is generated even when a response is served from the cache.

## Time Quota Calculations

Calculation of time quotas is as follows:

- HTTP and decrypted HTTPS traffic – The duration of each connection to the same URL category, from formation to disconnect, plus one minute, is counted toward the time quota limit. If multiple requests are made to the same URL category within one minute of each other, they are counted as one continuous session and the one minute is added only at the end of this session (that is, after at least one minute of "silence").
- Tunnel traffic (including tunneled HTTPS) – The actual duration of the tunnel, from formation to disconnect, counts toward quota limits. The above calculation for multiple requests applies to tunneled traffic as well.
- FTP – The actual duration of the FTP control session, from formation to disconnect, counts toward quota limits. The above calculation for multiple requests applies to FTP traffic as well.

## Defining Time and Volume Quotas

### Before you begin

- Go to **Security Services** > **Acceptable Use Controls** to enable Acceptable Use Controls.
- Define a time range unless you want the quota to apply as a daily limit.

### Procedure

**Step 1** Navigate to **Web Security Manager** > **Define Time Ranges and Quotas**.

**Step 2** Click **Add Quota**.

**Step 3** Enter a unique **Quota Name** in the field.

**Step 4** To reset the Time and Volume quota every day, select **Reset this quota daily at** and enter a time in the 12-hour format in the field, then choose **AM** or **PM** from the menu. Alternatively, select **Select a predefined time range profile**.

**Step 5** To set a time quota, select the **Time Quota** check box and choose the number of hours from the **hrs** menu and the number of minutes from the **mins** menu, from zero (always blocked) to 23 hours and 59 minutes.

**Step 6** To set a volume quota enter a number in the field and choose **KB** (kilobytes), MB (megabytes), or **GB** (gigabytes) from the menu.

**Step 7** Click **Submit** and then click **Commit Changes** to apply your changes. Alternatively, click **Cancel** to abandon your changes.

#### What to do next

(Optional) Navigate to **Security Services** > **End-User Notification** to configure end-user notifications for quotas.

# Access Control 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, 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 custom URL categories for host names 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.

See Creating and Editing Custom URL Categories, on page 183 for information about creating custom URL categories.

## Using URL Categories to Identify Web Requests

#### Before you begin

- Enable Acceptable Use Control, see Configuring the URL Filtering Engine , on page 168.
- (Optional) Create Custom URL Categories, see Creating and Editing Custom URL Categories, on page 183.

### Procedure

**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 , on page 168.
- (Optional) Create Custom URL Categories, see Creating and Editing Custom URL Categories, on page 183.



**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.

### Procedure

**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:

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 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, on page 238
- How to Configure Identification of Remote Users, on page 238
- Display Remote User Status and Statistics for ASAs, on page 240


## 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.

## How to Configure Identification of Remote Users

| Task | Further information |
|---|---|
| **1.** Configure identification of remote users. | Configuring Identification of Remote Users, on page 239 |
| **2.** Create an identity for remote users. | Classifying Users and Client Software, on page 131<br>**1.** In the “Define Members by User Location” section, select Remote Users Only.<br>**2.** In the “Define Members by Authentication” section, select “Identify Users Transparently through Cisco ASA Integration.” |

| Task | Further information |
|---|---|
| **3.** Create a policy for remote users. | Creating a Policy , on page 219 |

## Configuring Identification of Remote Users

### Procedure

**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. | **a.** Enter a range of IP addresses in the IP Range field.<br>**b.** 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. | **a.** Enter the Cisco ASA host name or IP address.<br>**b.** Enter the port number used to access the ASA. The default port number for the Cisco ASA is 11999.<br>**c.** If multiple Cisco ASA are configured in a cluster, click **Add Row** and configure each ASA in the cluster.<br>**Note** If two Cisco ASA are configured for high availability, enter only one host name or IP address for the *active* Cisco ASA.<br>**d.** Enter the access passphrase for the Cisco ASA.<br>**Note** The passphrase you enter here must match the access passphrase configured for the specified Cisco ASA.<br>**e.** Optional, click **Start Test** to verify the Web Security Appliance can connect to the configured Cisco ASA. |

**Step 4** Submit and Commit Changes.

**Note**
Enable AnyConnect Security Mobility (**Security Services** > **AnyConnect Security Mobility**) to make the Define Members by User Location option available on the Web Security Appliance . By default, this option is available on the Cisco Content Security Management Appliance (**Web** > **Configuration Master** > **Identification Profiles**). When you use the Define Members by User Location option to configure an identification profile in the Security Management Appliance

and publish that configuration to the Web Security Appliance where AnyConnect Security Mobility is not enabled, the identification profile is disabled.

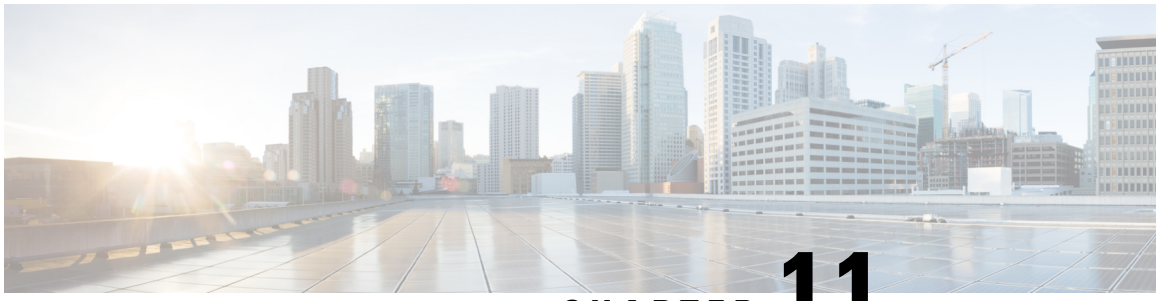
## Display Remote User Status and Statistics for ASAs

Use this command to display information related to Secure Mobility when the Web Security Appliance is integrated with an ASA.

| Command | Description |
|---|---|
| `musstatus` | This command displays the following information:<br>• The status of the Web Security Appliance connection with each ASA.<br>• The duration of the Web Security Appliance connection with each ASA in minutes.<br>• The number of remote clients from each ASA.<br>• 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 .<br>• The total number of remote clients. |

# Troubleshooting Policies


- Access Policy not Configurable for HTTPS, on page 571
- Some Microsoft Office Files Not Blocked, on page 558
- Blocking DOS Executable Object Types Blocks Updates for Windows OneCare, on page 559
- Identification Profile Disappeared from Policy, on page 572
- Policy is Never Applied, on page 572
- HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 572
- User Matches Global Policy for HTTPS and FTP over HTTP Requests, on page 573
- User Assigned Incorrect Access Policy , on page 573
- Policy Troubleshooting Tool: Policy Trace, on page 573



CHAPTER 11

# Create Decryption Policies to Control HTTPS Traffic

This topic contains the following sections:


- Overview of Create Decryption Policies to Control HTTPS Traffic, on page 241
- Managing HTTPS Traffic through Decryption Policies Best Practices, on page 242
- Decryption Policies , on page 242
- Root Certificates, on page 249
- Routing HTTPS Traffic, on page 256
- Troubleshooting Decryption/HTTPS/Certificates, on page 256


# Overview of Create Decryption Policies to Control HTTPS 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, on page 245 |
| 2 | Upload or Generate a certificate and key | • Uploading a Root Certificate and Key, on page 251<br>• Generating a Certificate and Key for the HTTPS Proxy, on page 252 |
| 3 | Configuring Decryption options | Configuring Decryption Options, on page 248 |
| 5 | (Optional) Configure invalid certificate handling | Configuring Invalid Certificate Handling, on page 252 |
| 6 | (Optional) Enabling real-time revocation status checking | Enabling Real-Time Revocation Status Checking, on page 254 |
| 7 | (Optional) Manage trusted and blocked certificates | Trusted Root Certificates, on page 255 |

# 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. |

| Option | Description |
|---|---|
| **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.<br><br>However, with a standard pass-through policy, the Web Security Appliance does check the validity of the requested server by initiating an HTTPS handshake with the server. This validity check includes server certificate validation. If the server fails the check, the transaction is blocked.<br><br>You can skip validation checks for specific sites by configuring policies that incorporate custom categories which include these sites, thereby indicating that these sites are trustworthy—these sites are passed through without validity checks. Exercise care when configuring policies that allow validity checks to be skipped. |
| **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. |

All actions except Monitor are “final actions” the Web Proxy applies to a transaction. A final action is an action that causes the Web Proxy to stop evaluating the transaction against other control settings. For example, if a Decryption Policy is configured to monitor invalid server certificates, the Web Proxy makes no final decision on how to handle the HTTPS transaction if the server has an invalid certificate. If a Decryption Policy is configured to block servers with a low Web reputation score, then any request to a server with a low reputation score is dropped without considering the URL category actions.

The following diagram shows how the Web Proxy evaluates a client request against the Decryption Policy groups. Applying Decryption Policy Actions shows the order the Web Proxy uses when evaluating control settings for Decryption Policies. Figure 5: Applying Access Policy Actions, on page 231 shows the order the Web Proxy uses when evaluating control settings for Access Policies.

*Figure 6: Applying Decryption Policy Actions*

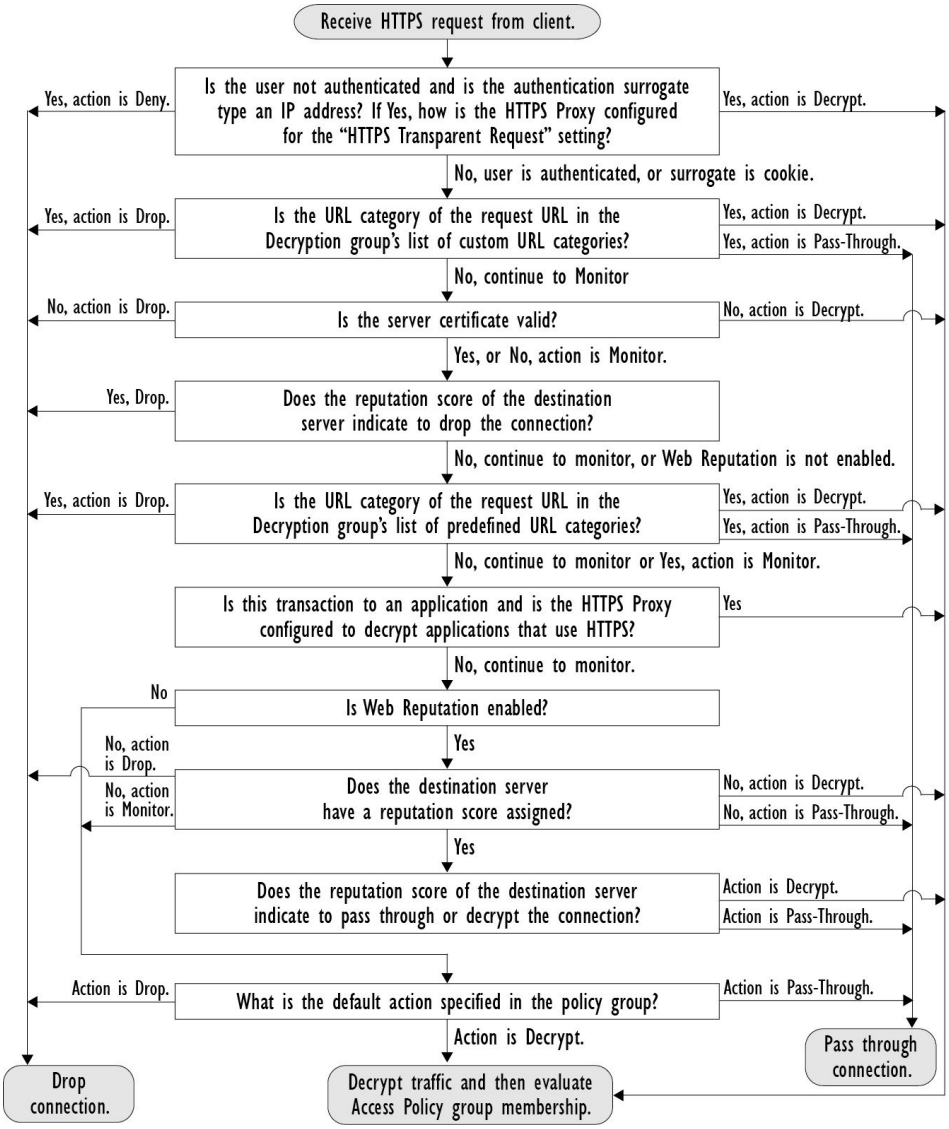
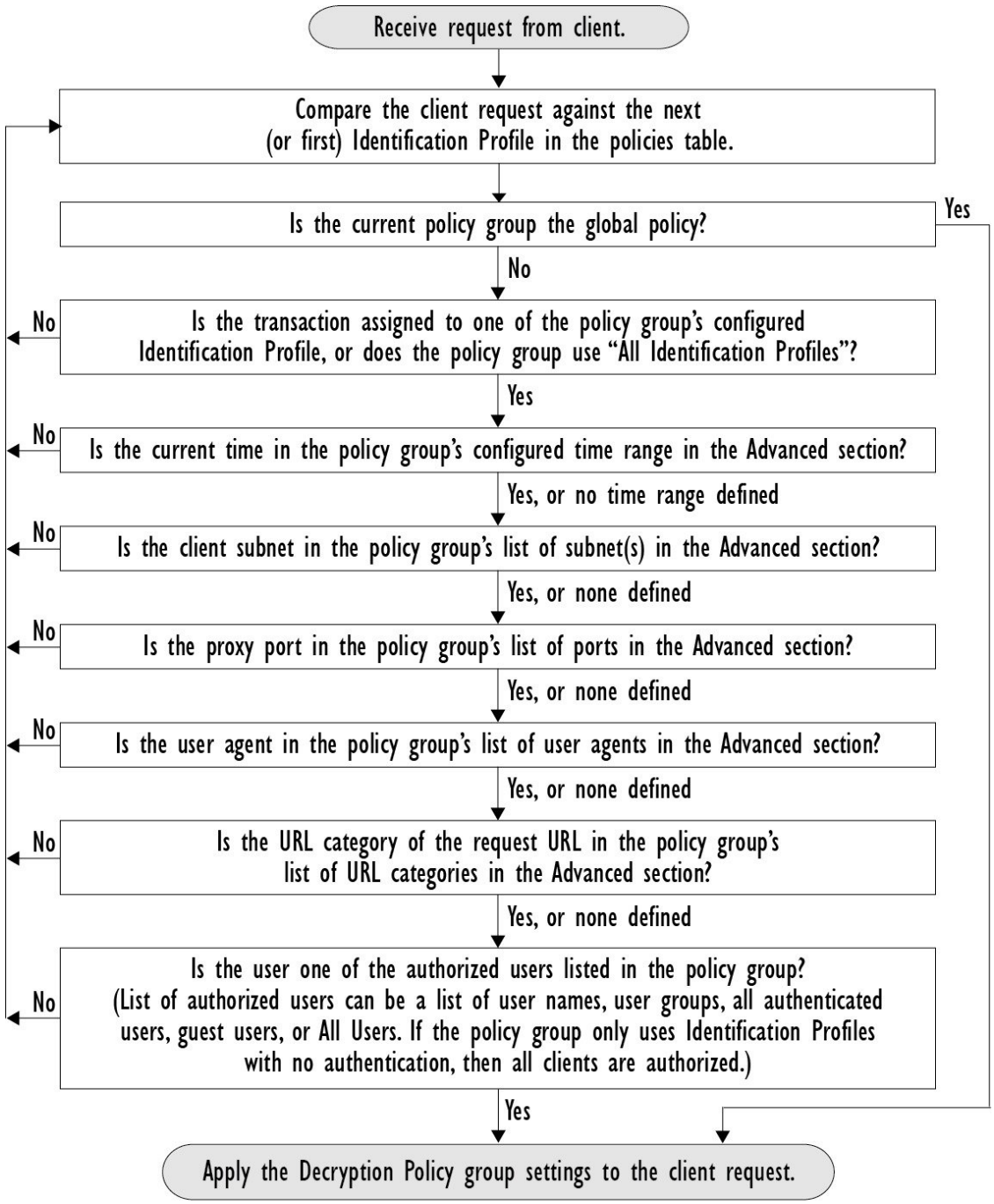


*Figure 7: Policy Group Transaction Flow for Decryption Policies*




# 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.

## Procedure

**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**
Web Security Appliance can use maximum of 30 ports as proxy:3 ports are always reserved for FTP proxy, and 27 ports can be configured as HTTP and HTTPS proxy.

**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** **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 Managing Certificate Validation and Decryption for HTTPS, on page 250.

**Step 8** Submit and commit your changes.

### What to do next

### Related Topics

- Managing Certificate Validation and Decryption for HTTPS, on page 250

# Controlling HTTPS Traffic

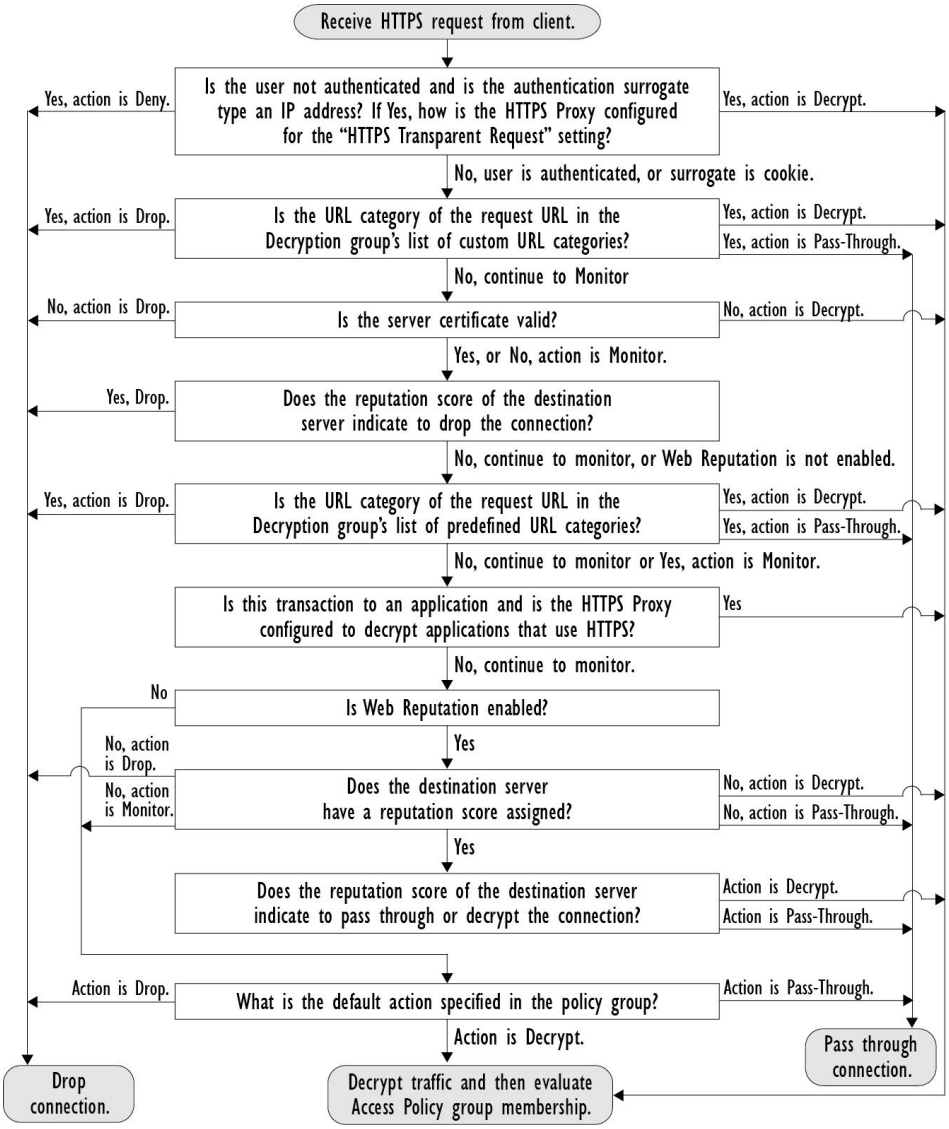
After the Web Security Appliance assigns an HTTPS connection request to a Decryption Policy group, the connection request inherits the control settings of that policy group. The control settings of the Decryption Policy group determine whether the appliance decrypts, drops, or passes through the connection:

| Option | Description |
|---|---|
| **URL Categories** | You can configure the action to take on HTTPS requests for each predefined and custom URL category. Click the link under the URL Filtering column for the policy group you want to configure.<br>**Note**<br>If you want to *block* (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. |
| **Web Reputation** | 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. |
| **Default Action** | 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.<br>**Note**<br>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. |

To bypass encrypted traffic having a good web reputation score, make sure that you disable the **Decrypt for Application Detection** option in the **Decryption Options** section of the HTTPS Proxy Settings page.

The following diagram shows how the appliance determines which action to take on an HTTPS request after it has assigned a particular Decryption Policy to the request. The Web reputation score of the destination server is evaluated only once, but the result is applied at two different points in the decision flow. For example, note that a Web reputation score Drop action overrides any action specified for predefined URL categories.

*Figure 8: Applying Decryption Policy Actions*




# Configuring Decryption Options

### Before you begin

Verify that the HTTPS proxy is enabled as described in Enabling the HTTPS Proxy, on page 245.

### Procedure

**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.<br>**Note**<br>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 Acknowledgment | For users who have not acknowledged the web proxy prior to this HTTPS transaction, allow decryption so that AsyncOS can display the end-user acknowledgment. |
| 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 | • secure client authentication disabled or<br>• secure client authentication enabled and an IP-based surrogate |
| Transparent requests | • IP-based surrogate, decryption for authentication enabled or<br>• IP-based surrogate, client previously authenticated using an HTTP request |

# Root 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. See About Certificates and Keys, on page 534 for more information.

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.

### Procedure

**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

- Enabling Real-Time Revocation Status Checking, on page 254
- Configuring Invalid Certificate Handling, on page 252
- Options for Certificate Revocation Status Checking, on page 253

## 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, on page 245.

### Procedure

**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.

**Step 9** Submit and commit your changes.

# Generating a Certificate and Key for the HTTPS Proxy

### Before you begin

Enable the HTTPS Proxy. Enabling the HTTPS Proxy, on page 245.

### Procedure

**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, on page 245.

### Procedure

**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.<br>**Note**<br>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, on page 254
- Configuring Invalid Certificate Handling, on page 252

## Enabling Real-Time Revocation Status Checking

### Before you begin

Ensure the HTTPS Proxy is enabled. See Enabling the HTTPS Proxy, on page 245.

### Procedure

**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. |

| Field Name | Description |
|---|---|
| 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 primary 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, on page 245.

### Procedure

**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

### Procedure

**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.

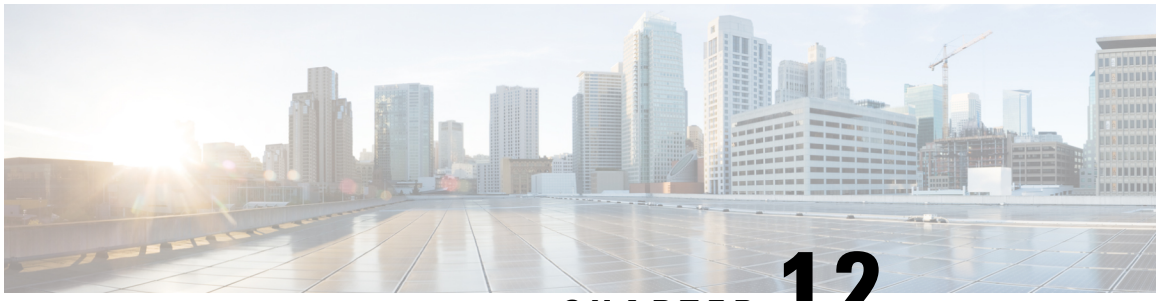
# Routing HTTPS Traffic

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 if any routing policy or identification profile relies on the information in client headers. |
| Explicit HTTPS | In the case of explicit HTTPS, AsyncOS has access to the following information in client headers:<br>• URL<br>• Destination port number<br>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, on page 563
- HTTPS with IP-based Surrogates and Transparent Requests, on page 563
- Bypassing Decryption for Particular Websites, on page 564
- Alert: Problem with Security Certificate, on page 565



CHAPTER 12

# Scan Outbound Traffic for Existing Infections

This topic contains the following sections:


- Overview of Scanning Outbound Traffic, on page 257
- Understanding Upload Requests, on page 258
- Creating Outbound Malware Scanning Policies, on page 259
- Controlling Upload Requests , on page 261
- Logging of DVS Scanning, on page 262


## 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 Dynamic Vectoring and Streaming (DVS) engine scans transaction requests as they leave the network. By working with the Cisco 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, on page 259 |
| Assign upload requests to outbound malware policy groups | Controlling Upload Requests , on page 261 |

## User Experience When Requests Are Blocked by the DVS Engine

When the Cisco 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 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 |
|---|---|
| **Identification Profile** | Each client request either matches an **Identification Profile**, fails authentication and is granted guest access, or fails authentication and is terminated. |
| **Authorized users** | If the assigned **Identification Profile** 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 **Identification Profile** 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 **Identification Profile**. When an advanced option is configured in the **Identification Profile**, 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.

### Procedure

**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 **Identification Profiles** 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 | Choose whether or not to define policy group membership by the protocol used in the client request. Select the protocols to include.<br>"All others" means any protocol not listed above this option.<br>**Note**<br>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. |

| Advanced Option | Description |
|---|---|
| Proxy Ports | 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.<br>For explicit forward connections, this is the port configured in the browser. For transparent connections, this is the same as the destination port.<br>If you define policy group membership by the proxy port when client requests are transparently redirected to the appliance, some requests might be denied.<br>**Note**<br>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. |
| Subnets | Choose whether or not to define policy group membership by subnet or other addresses.<br>You can select to use the addresses that may be defined with the associated Identity, or you can enter specific addresses here.<br>**Note**<br>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. |
| URL Categories | Choose whether or not to define policy group membership by URL categories. Select the user defined or predefined URL categories.<br>**Note**<br>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. |
| User Agents | Choose whether to define policy group membership by the user agents (client applications such as updaters and Web browsers) used in the client request. You can select some commonly defined user agents, or define your own using regular expressions. Specify whether membership definition includes only the selected user agents, or specifically excludes the selected user agents.<br>**Note**<br>If the **Identification Profile** associated with this policy group defines **Identification Profile** membership by this advanced setting, the setting is not configurable at the non-**Identification Profile** policy group level. |
| User Location | Choose whether or not to define policy group membership by user location, either remote or local. |

**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.

### Procedure

**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.<br>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 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 of DVS Scanning

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:

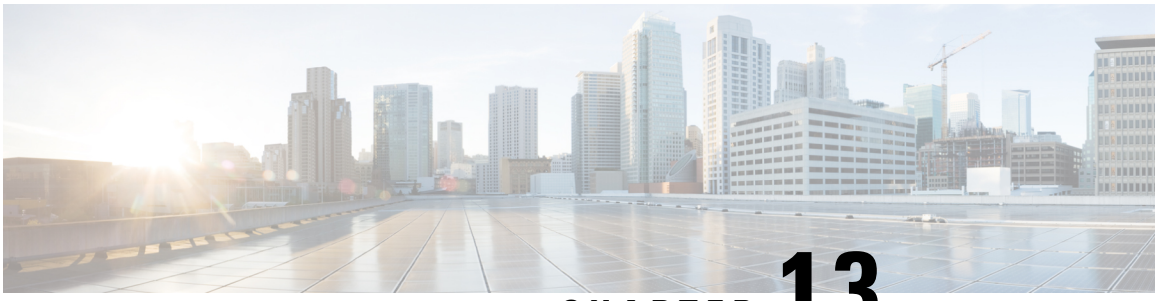
***Table 6: Log Fields in W3C Logs and Format Specifiers in Access Logs***

| 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.



CHAPTER 13

# Configuring Security Services

This topic contains the following sections:


- Overview of Configuring Security Services , on page 263
- Overview of Web Reputation Filters , on page 264
- Overview of Anti-Malware Scanning , on page 266
- Understanding Adaptive Scanning, on page 269
- Enabling Anti-Malware and Reputation Filters, on page 269
- Configuring Anti-Malware and Reputation in Policies, on page 271
- Integrating the Appliance with AMP for Endpoints Console, on page 276
- Maintaining the Database Tables, on page 278
- Logging of Web Reputation Filtering Activity and DVS Scanning , on page 278
- Caching, on page 279
- Malware Category Descriptions, on page 279


## 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 , on page 266 |
| Web Reputation Filters | Analyzes web server behavior and determines whether the URL contains URL-based malware | Overview of Web Reputation Filters , on page 264 |
| 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 , on page 281 |

**Related Topics**

- Enabling Anti-Malware and Reputation Filters, on page 269
- Understanding Adaptive Scanning, on page 269

# 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 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, passphrases, 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 |

| Policy Type | Action |
|---|---|
| **Decryption Policies** | You can choose to drop, decrypt, or pass through |
| **Cisco 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. | • URL downloads information without user permission.<br>• Sudden spike in URL volume.<br>• 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. | • Recently created URL that has a dynamic IP address and contains downloadable content.<br>• 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. | • URL contains no downloadable content.<br>• Reputable, high-volume domain with long history.<br>• Domain present on several allow lists.<br>• 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 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, on page 269

## 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. |

| Score | Action | Description |
|---|---|---|
| 6.0 to 10.0 | Pass through | Good site. Request is passed through with no inspection or decryption. |

### Web Reputation in Cisco 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).<br>**Note**<br>Sites with no score are monitored. |

# Overview of Anti-Malware Scanning

The Web Security Appliance  anti-malware feature uses the Cisco 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 Anti-Malware and Reputation Filters, on page 269
- Understanding Adaptive Scanning, on page 269
- McAfee Scanning, on page 267

# 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.

### Procedure

**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. |

| Setting | Description |
|---|---|
| File Reputation Filtering and File Analysis | See Enabling and Configuring File Reputation and Analysis Services. |
| AMP for Endpoints Console Integration (**Advanced** > **Advanced Settings for File Reputation**) | Click **Register the Appliance with** AMP for Endpoints to integrate your appliance with AMP for Endpoints console. For detailed instructions, see Integrating the Appliance with AMP for Endpoints Console, on page 276. |
| DVS Engine Object Scanning Limits | Specify a maximum object size for scanning.<br>The Maximum Object Size value you specify applies to the entire size of requests and responses that might be scanned by all anti-malware and anti-virus scanning engines and by Advanced Malware Protection features. It also specifies the maximum size of an inspectable archive for Archive inspection; see Access Policies: Blocking Objects, on page 226 for more about Archive inspection.<br>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. If an inspectable archive exceeds this size, it is marked "Not Scanned." |
| Sophos | Choose whether or not to enable the Sophos scanning engine. |
| McAfee | Choose whether or not to enable the McAfee scanning engine.<br>When you enable the McAfee scanning engine, you can choose whether or not to enable heuristic scanning.<br>**Note**<br>Heuristic analysis increases security protection, but can result in false positives and decreased performance. |
| Webroot | Choose whether or not to enable the Webroot scanning engine.<br>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.<br>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.<br>**Note**<br>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. |

**Step 4** Submit and Commit Changes.

### What to do next

- Understanding Adaptive Scanning, on page 269

- McAfee Scanning, on page 267

# Clearing the  Advanced Malware Protection Services Cache

AMP clear cache functionality clears file reputation dispositions for clean, malicious, and unknown files.

**Note** AMP cache is used to increase performance. By using **Clear Cache** command, you might observe a temporary performance degradation while the cache is repopulated.

### Procedure

**Step 1** Choose **Security Services** > **Anti-Malware and Reputation**.

**Step 2** In the  Advanced Malware Protection Services section, click **Clear Cache** and confirm your action.

# 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** | Anti-Malware and Reputation Settings in Access Policies, on page 272 |
| **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** | Anti-Malware and Reputation Settings in Access Policies, on page 272 |
| **Decryption Policies** | Configuring Web Reputation Filter Settings for Decryption Policy Groups, on page 275 |
| **Cisco Data Security Policies** | Configuring Web Reputation Filter Settings for Decryption Policy Groups, on page 275 |

You can configure  Advanced Malware Protection settings only in Access Policies. See Configuring File Reputation and Analysis Features, on page 285

# 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 Primary Configuration, options on this page depend on whether Adaptive Security is enabled for the relevant primary configuration. Check the setting on the Security Management appliance, on the **Web > Utilities > Security Services Display** page.

• Understanding Adaptive Scanning, on page 269

## Configuring Anti-Malware and Reputation Settings with Adaptive Scanning Enabled

### Procedure

**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.

| | |
|---|---|
| Enable Suspect User Agent Scanning | Choose whether or not to scan traffic based on the user-agent field specified in the HTTP request header.<br>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.<br>**Note**<br>Chrome browsers do not include a user-agent string in FTP-over-HTTP requests; therefore, Chrome cannot be detected as the user agent in those requests. |
| 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.<br>**Note**<br>The category Outbreak Heuristics applies to transactions which are identified as malware by Adaptive Scanning prior to running any scanning engines.<br>**Note**<br>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.

### What to do next

- Understanding Adaptive Scanning, on page 269

## Configuring Anti-Malware and Reputation Settings with Adaptive Scanning Disabled

### Procedure

**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.<br>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.<br>**Note**<br>Chrome browsers do not include a user-agent string in FTP-over-HTTP requests; therefore, Chrome cannot be detected as the user agent in those requests. |
| 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.<br>**Note**<br>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.

### What to do next

- Configuring Web Reputation Score Thresholds for Access Policies, on page 274
- Malware Category Descriptions, on page 279

# 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

### Procedure

**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

### Procedure

**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

### Procedure

**Step 1** Choose **Web Security Manager** > **Cisco 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 Data Security Policies. By definition, all positive scores are monitored

# Integrating the Appliance with AMP for Endpoints Console

You can integrate your appliance with AMP for Endpoints console, and perform the following actions in AMP for Endpoints console:

- Create a simple custom detection list.
- Add new malicious file SHAs to the simple custom detection list.
- Create an application allowed list.
- Add new file SHAs to the application allowed list.
- Create a custom policy.
- Attach the simple custom detection list and the application allowed list to the custom policy.
- Create a custom group.
- Attach the custom policy to the custom group.
- Move your registered appliance from the default group to the custom group.
- View the file trajectory details of a particular file SHA.

To integrate your appliance with AMP for Endpoints console, you need to register your appliance with the console.

After the integration, when a file SHA is sent to the File Reputation server, the verdict obtained for the file SHA from the File Reputation Server is overridden by the verdict already available for the same file SHA in the AMP for Endpoints console.

If a file SHA is already marked as malicious globally, and if the same file SHA is added to the blocked list in AMP for Endpoints console, the file disposition is malicious.

The Advanced Malware Protection report page includes a new section - **Incoming Malware Files by Category** to view the percentage of block listed file SHAs received from the AMP for Endpoints console that are displayed as **Custom Detection**. The threat name of a block listed file SHA is displayed as **Simple Custom Detection** in the Incoming Malware Threat Files section of the report. You can click the link in the More Details section of the report to view the file trajectory details of a block listed file SHA in the AMP for Endpoints console.

The Advanced Malware Protection report page includes a new section - **Incoming Malicious Files by Category** to view the percentage of file SHAs on the blocked list received from the AMP for Endpoints console that are displayed as **Custom Detection**. The threat name of a file SHA on the blocked list is displayed as **Custom Detection** in the Malicious Threat Files section of the report. To view the file trajectory details about a file SHA on the blocked list in the AMP for Endpoints console, see #unique_452.

### Before you begin

Make sure you have a user account in AMP for Endpoints console with admin access rights. For more details on how to create an AMP for Endpoints console user account, contact Cisco TAC.

[For clustered configuration] In a clustered configuration, you can only register your logged-in appliance with AMP for Endpoints console. If you have already registered your appliance with AMP for Endpoints console in the standalone mode, make sure to deregister the appliance manually before you join it to a cluster.

Make sure you have enabled and configured File Reputation Filtering. See Enabling and Configuring File Reputation and Analysis Services to know how to enable and configure File Reputation Filtering.

### Procedure

**Step 1** Select **Security Services > Anti-Malware and Reputation**.

**Step 2** Click **Edit Global Settings**.

**Step 3** Click **Register Appliance with** AMP for Endpoints in the Advanced Settings panel for File Reputation in the File Reputation and File Analysis page of the web interface.

Once you click Register Appliance with AMP for Endpoints, the AMP for Endpoints console login page appears.

**Step 4** Click **Register Appliance with** AMP for Endpoints in the Advanced Settings panel for File Reputation in the Anti-Malware Reputation page of the web interface.

Once you click Register Appliance with AMP for Endpoints, the AMP for Endpoints console login page appears.

**Note**
You must enable and configure File Reputation Filtering before you register the appliance with AMP for Endpoints. See Enabling and Configuring File Reputation and Analysis Services to know how to enbale and configure File Reputaion Filtering.

**Step 5** Log in to the AMP for Endpoints console with your user credentials.

**Step 6** Click **Allow** in the AMP for Endpoints authorization page to register your appliance.

Once you click Allow, the registration is complete, and it redirects you to the Anti-Malware Reputation page of your appliance. Your appliance name is displayed in the AMP for Endpoints Console Integration field. You can use the appliance name to customize your appliance settings in the AMP for Endpoints console page.

### What to do next

**Next Steps**:

- You can go to Accounts > Applications section of the AMP for Endpoints console page, to verify whether your appliance is registered with AMP for Endpoints console. Your appliance name is displayed in the Applications section of the AMP for Endpoints console page.
- After registration, your appliance is added to the default group (Audit Group) which has a default policy (Network Policy) attached to it. The default policy contains file SHAs that are added to the blocked list or the allowed list. If you want to customize the AMP for Endpoints settings for your appliance, and add your own file SHAs that are added to the blocked list or the allowed list, see the AMP for Endpoints user documentation at https://console.amp.cisco.com/docs.
- To deregister your appliance connection from AMP for Endpoints console, you can click **Deregister** in the Advanced Settings for File Reputation section in your appliance, or you need to go to the AMP for Endpoints console page at https://console.amp.cisco.com/. For more information, see the AMP for Endpoints user documentation at https://console.amp.cisco.com/docs.

**Note** When you change your File Reputation server to a different data center, your appliance is automatically deregistered from the AMP for Endpoints console. You must re-register your appliance with AMP for Endpoints console with the same data center selected for the File Reputation server.

**Note** If a malicious file SHA gets a clean verdict, then verify whether the same file SHA is added to the allowed list in AMP for Endpoints console.

# Maintaining the Database Tables

The web reputation, Webroot, Sophos, and McAfee databases periodically receive updates from the Cisco update server. 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 of Web Reputation Filtering Activity and DVS Scanning

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

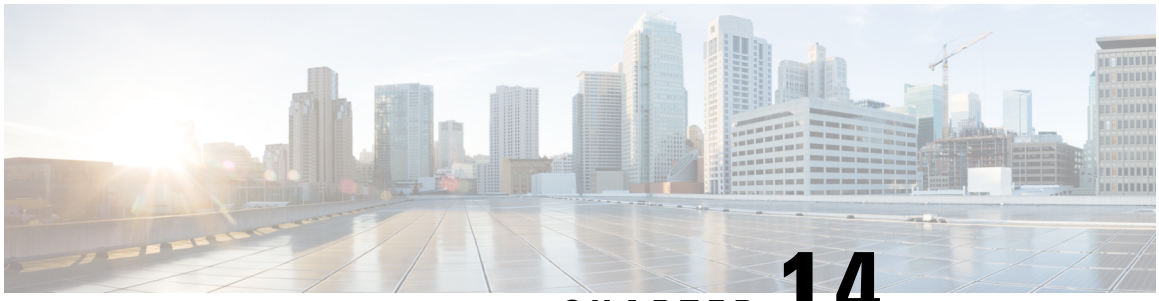
The following guidelines explain how AsyncOS uses the cache while scanning for malware:

- 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. |

| Malware Type | Description |
|---|---|
| System Monitor | A system monitor encompasses any software that performs one of the following:<br>• Overtly or covertly records system processes and/or user action.<br>• 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 passphrases. |
| 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. |



CHAPTER 14

# File Reputation Filtering and File Analysis

This chapter contains the following sections:


- Overview of File Reputation Filtering and File Analysis , on page 281
- Configuring File Reputation and Analysis Features, on page 285
- File Reputation and File Analysis Reporting and Tracking , on page 295
- Taking Action When File Threat Verdicts Change , on page 298
- Troubleshooting File Reputation and Analysis , on page 299


# Overview of File Reputation Filtering and File Analysis

Advanced Malware Protection protects against zero-day and targeted file-based threatsby:

- Obtaining the reputation of known files.
- Analyzing behavior of certain files that are not yet known to the reputation service.
- Continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.

This feature is available for file downloads. Uploaded files.

The file reputation and file analysis services have options for either public- or private-cloud (on-premesis).

- The private-cloud file reputation service is provided by Cisco AMP Virtual Private Cloud appliance, operating in either “proxy” or “air-gap” (on-premises) mode. See Configuring an On-premises File Reputation Server, on page 287.
- The private-cloud file analysis service is provided by an on-premises Cisco AMP Malware Analytics appliance. See Configuring an On-Premises File Analysis Server , on page 287.

## File Threat Verdict Updates

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 as new information becomes available, 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.

Information about the timing of verdict updates is included in the file-criteria document referenced in Supported Files for File Reputation and Analysis Services , on page 283.

### Related Topics

- File Reputation and File Analysis Reporting and Tracking , on page 295
- Taking Action When File Threat Verdicts Change , on page 298

# File Processing Overview

First, the website 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:

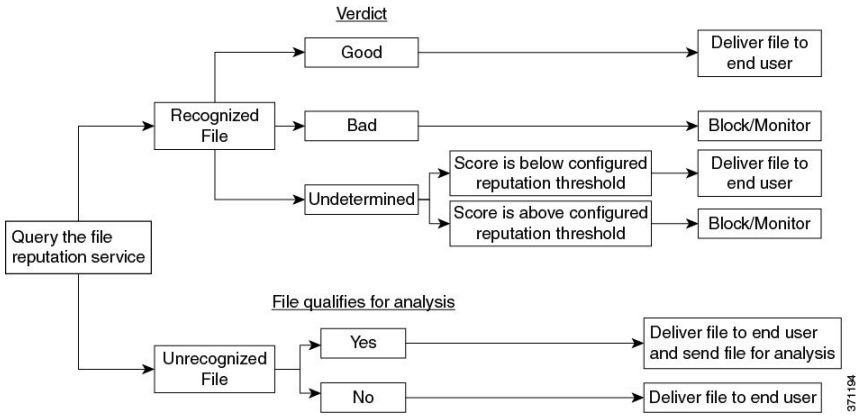
- If the file is known to the file reputation service and is determined to be clean, the file is released to the end user .
- If the file reputation service returns a verdict of malicious, then the appliance applies the action that you have specified for such files.
- If the file is known to the reputation 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, 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 (see Supported Files for File Reputation and Analysis Services , on page 283), the file is considered clean and the file is released to the end user .
- If you have enabled the cloud-based File Analysis service, and the reputation service has no information about the file, and the file meets the criteria for files that can be analyzed (see Supported Files for File Reputation and Analysis Services , on page 283), then the file is considered clean and is optionally sent for analysis.
- For deployments with on-premises file analysis, the reputation evaluation and file analysis occur simultaneously. If the reputation service returns a verdict, that verdict is used, as the reputation service includes inputs from a wider range of sources. If the file is unknown to the reputation service, the file is released to the user but the file analysis result is updated in the local cache and is used to evaluate future instances of the file .

- If the file reputation verdict information is unavailable because the connection with the server timed out, the file is considered as Unscannable and the actions configured are applied.

### Low Risk Files

When a file is initially evaluated as unknown, and has no dynamic content, the appliance sends it to the pre-classification engine, where it is designated as low risk. This file is not uploaded for analysis. If the same file is accessed within the cache expiry, it is evaluated again as low risk, and is not uploaded for analysis. After the cache timeout, if the same file is accessed again, it is evaluated as unknown and low risk sequentially. This process is repeated for low risk files. Since these low risk files are not uploaded, they will not be a part of file analysis reports.

***Figure 9: Advanced Malware Protection Workflow for Cloud File Analysis Deployments***




If the file is sent for analysis:

- If the file is sent to the cloud for analysis: Files are sent over HTTPS.
- Analysis normally takes minutes, but may take longer.
- A file that is flagged as malicious after File Analysis may not be identified as malicious by the reputation service. File reputation is determined by a variety of factors over time, not necessarily by a single file analysis verdict.
- Results for files analyzed using an on premises Cisco Secure Endpoint Malware Analytics appliance are cached locally.

For information about verdict updates, see File Threat Verdict Updates , on page 281.

# Supported Files for File Reputation and Analysis Services

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. When you configure the file analysis feature, you choose which file types are analyzed. New types can be added dynamically; you will receive an alert when the list of uploadable file types changes, and can select added file types to upload.

Details about what files are supported by the reputation and analysis services are available only to registered Cisco customers. For information about which files are evaluated and analyzed, see *File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*, available from

http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html. The criteria for evaluating a file's reputation and for sending files for analysis may change at any time.

In order to access this document, you must have a Cisco customer account with a support contract. To register, visit https://tools.cisco.com/RPF/register/register.do.

Your setting for **DVS Engine Object Scanning Limits** on the **Security Services > Anti-Malware and Reputation** page also determines the maximum file size for file reputation and analysis.

You should configure policies to block download of files that are not addressed by Advanced Malware Protection.



**Note** A file that has already been uploaded for analysis from any source will not be uploaded again. To view analysis results for such a file, search for the SHA-256 from the File Analysis reporting page.

### Related Topics

- Enabling and Configuring File Reputation and Analysis Services , on page 288
- Ensuring That You Receive Alerts About Advanced Malware Protection Issues, on page 294
- Archive or Compressed File Processing, on page 284

## Archive or Compressed File Processing

If the file is compressed or archived,

- Reputation of the compressed or archive file is evaluated.
- In case of some selective file types, the compressed or archive file is decompressed and reputations of all the extracted files are evaluated.

For information about which archived and compressed files are examined, including file formats, see the information linked from Supported Files for File Reputation and Analysis Services , on page 283.

In this scenario,

- If one of the extracted files is malicious, the file reputation service returns a verdict of Malicious for the compressed or the archive file.
- If the compressed or archive file is malicious and all the extracted files are clean, the file reputation service returns a verdict of Malicious for the compressed or the archive file.
- If the verdict of any of the extracted files is unknown, the extracted files are optionally (if configured and the file type is supported for file analysis) sent for file analysis.
- If the extraction of a file fails while decompressing a compressed or an archive file, the file reputation service returns a verdict of Unscannable for the compressed or the archive file. Keep in mind that, in this scenario, if one of the extracted files is malicious, the file reputation service returns a verdict of Malicious for the compressed or the archive file (Malicious verdict takes precedence over Unscannable verdict).
- An compressed or archive file is treated as unscannable in the following scenarios:
  - The data compression ratio is more than 20.

- The archive file contains more than five levels of nesting.
- The archive file contains more than 200 child files.
- The archive file size is more than 50 MB.
- The archive file is password protected or unreadable.



**Note** Secure Web Appliance sends the entire archive file to Cisco Secure Malware Analytics if one or more constituent files qualify for File Analysis. The entire archive file is marked malware if any constituent files are found malicious.

If the Secure Web Appliance fails to extract a compressed or archive file, it will be uploaded to Secure Malware Analytics for analysis.



**Note** Reputation of the extracted files with safe MIME types, for example, text/plain, are not evaluated.

## Privacy of Information Sent to the Cloud

- Only the SHA that uniquely identifies a file is sent to the reputation service in the cloud. The file itself is not sent.
- If you are using the file analysis service in the cloud and a file qualifies for analysis, the file itself is sent to the cloud.
- Information about every file that is sent to the cloud for analysis and has a verdict of "malicious" is added to the reputation database. This information is used along with other data to determine a reputation score.

  Information about files analyzed by an on premises Cisco Secure Endpoint Malware Analytics appliance is not shared with the reputation service.

# Configuring File Reputation and Analysis Features


- Requirements for Communication with File Reputation and Analysis Services , on page 286
- Configuring an On-premises File Reputation Server, on page 287
- Configuring an On-Premises File Analysis Server , on page 287
- Enabling and Configuring File Reputation and Analysis Services
- (Public Cloud File Analysis Services Only) Configuring Appliance Groups , on page 292
- Configuring File Reputation and Analysis Service Action Per Access Policy , on page 294
- Ensuring That You Receive Alerts About Advanced Malware Protection Issues, on page 294
- Configuring Centralized Reporting for Advanced Malware Protection Features , on page 295

# Requirements for Communication with File Reputation and Analysis Services

- All that use these services must be able to connect to them directly over the internet (excluding File Analysis services configured to use an on-premises Cisco Secure Endpoint Malware Analytics Appliance.)
- 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 , on page 286.
- Using of a combination of public cloud servers and private/on-premis for file reputation and file analysis is not supported. If you are using an on-premis device, then both file analysis and reputation must have an on-premis cloud server. If you are using a public cloud server, then both file reputation and file analysis must have a public cloud server.
- By default, communication with file reputation and cloud-based analysis services is routed through the interface that is associated with the default gateway. To route this traffic through a different interface, create a static route for each address in the Advanced section of the Security Services > File Reputation and Analysis page.
- When you configure the file reputation feature, choose whether to use SSL over port 443.

### Related Topics

- Enabling and Configuring File Reputation and Analysis Services

## 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, on page 39

| For Connection To | Destination Network | Gateway |
|---|---|---|
| The file reputation service | In Security Services > Anti-Malware and Reputation, Advanced section > Advanced Settings for File Reputation section, provide the name (URL) of the **File Reputation Server**, and the cloud server pool's **Cloud Domain** name.<br><br>If you choose Private Cloud for File Reputation Server, enter the host name or IP address of the Server, and provide a valid Public Key. This must be the same key used by the private cloud appliance.<br><br>Host name of the Cloud Server Pool, as configured in Security Services ; Anti-Malware and Reputation, Advanced section: Advanced Settings for File Reputation. | IP address of the gateway for the data port |

| For Connection To | Destination Network | Gateway |
|---|---|---|
| The file analysis service | • In Security Services > Anti-Malware and Reputation, Advanced section > Advanced Settings for File Analysis section, provide the name (URL) of the **File Analysis Server**.<br>If you choose Private Cloud for the File Analysis Server, enter the Server URL, and provide a valid Certificate Authority.<br>• The File Analysis Client ID is client ID for this appliance on the File Analysis server (read-only).<br>Host name of the File Analysis Server, as configured in Security Services; Anti-Malware and Reputation, Advanced section: Advanced Settings for File Analysis. | IP address of the gateway for the data port |

**Related Topics**

- Configuring TCP/IP Traffic Routes, on page 39

# Configuring an On-premises File Reputation Server

If you will use a Cisco  AMP Virtual Private Cloud appliance as a private-cloud file analysis server:

- You can obtain the Cisco  Advanced Malware Protection Virtual Private Cloud Appliance documentation, including the Installation and Configuration of FireAMP Private Cloud guide, from http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html

  Use that documentation to perform the tasks described in this topic.

  Additional documentation is available using the Help link in the  AMP Virtual Private Cloud appliance.
- Set up and configure the Cisco  AMP Virtual Private Cloud appliance in either “proxy” or “air-gap” (on-premises) mode.
- Ensure the Cisco  AMP Virtual Private Cloud appliance software version is 2.2, which enables integration with Cisco .
- Download the  AMP Virtual Private Cloud certificate and keys on that appliance for upload to this

**Note** After you have set up the on-premises file-reputation server, you will configure connection to it from this ; see Step 6 of Enabling and Configuring File Reputation and Analysis Services , on page 288

# Configuring an On-Premises File Analysis Server

If you will use a Cisco Secure Endpoint Malware Analytics Appliance as a private-cloud file analysis server:

- Obtain the Cisco Secure Endpoint Malware Analytics Appliance Setup and Configuration Guide and the Cisco Secure Endpoint Malware Analytics Appliance Administration Guide. Cisco Secure Endpoint Malware Analytics Appliance documentation is available from https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html.

  Use this documentation to perform the tasks described in this topic.

  Additional documentation is available from the Help link in the Cisco Secure Endpoint Malware Analytics appliance.

  In the Administration Guide, search for information about all of the following: integrations with other Cisco appliances, CSA, Cisco Sandbox API .

- Set up and configure the Cisco Secure Endpoint Malware Analytics Appliance.
- If necessary, update your Cisco Secure Endpoint Malware Analytics Appliance software to version 1.2.1, which supports integration with Cisco.

  See the  AMP Malware Analytics documentation for instructions for determining the version number and for performing the update.

- Ensure that your appliances can communicate with each other over your network. Cisco must be able to connect to the CLEAN interface of the Cisco Secure Endpoint Malware Analytics appliance.
- If you will deploy a self-signed certificate: Generate a self-signed SSL certificate from the Cisco Secure Endpoint Malware Analytics appliance to be used on your . See instructions for downloading SSL certificates and keys in the administrator's guide for your Cisco Secure Endpoint Malware Analytics appliance. Be sure to generate a certificate that has the hostname of your Cisco Secure Endpoint Malware Analytics appliance as CN. The default certificate from the Cisco Secure Endpoint Malware Analytics appliance does NOT work.
- Registration of your with your Malware Analytics appliance occurs automatically when you submit the configuration for File Analysis, as described in  Enabling and Configuring File Reputation and Analysis Services. However, you must activate the registration as described in the same procedure.



**Note** After you have set up the on-premises file-analysis server, you will configure connection to it from this ; see Step 7 of  Enabling and Configuring File Reputation and Analysis Services

# Enabling and Configuring File Reputation and Analysis Services

### Before you begin

- Acquire feature keys for the file reputation service and the file analysis service and transfer them to this appliance. See Working with Feature Keys, on page 493 for more information about adding feature keys to the appliance.
- Meet the Requirements for Communication with File Reputation and Analysis Services , on page 286.
- Ensure that a Data network interface is enabled on the appliance if you want to use a Data network interface for File Reputation and Analysis services. See Enabling or Changing Network Interfaces, on page 24

- Verify connectivity to the update servers configured in Configuring Upgrade and Service Update Settings, on page 545.
- If you will use a Cisco  AMP Virtual Private Cloud Appliance as a private cloud file reputation server, see Configuring an On-premises File Reputation Server, on page 287.
- If you will use a Cisco Secure Endpoint Malware Analytics Appliance as a private cloud file analysis server, see Configuring an On-Premises File Analysis Server , on page 287.

## Procedure

**Step 1** Select **Security Services** > **Anti-Malware and Reputation**.

**Step 2** Click **Edit Global Settings**.

**Step 3** Click **Enable File Reputation Filtering** and optionally **Enable File Analysis**.

- If **Enable File Reputation Filtering** is checked, you must configure the section **File Reputation Server** (in **Step 6**), by either choosing the URL of an external public-reputation cloud server, or by providing the Private reputation cloud server connection information.
- Similarly, if **Enable File Analysis** is checked, you must configure the section **File Analysis Server URL** (in **Step 7**), providing either the URL of an external cloud server, or the Private analysis cloud connection information.

**Note**
New file types may be added after an upgrade and are not enabled by default. If you have enabled file analysis, and require the new file types to be included in analysis, you must enable them.

**Step 4** Accept the license agreement if presented.

**Step 5** In the **File Analysis** section, select the required file types from the appropriate file groups (for example, “Microsoft Documents”) to send for file analysis.

For information about supported file types, see the document described in Supported Files for File Reputation and Analysis Services , on page 283

**Step 6** Expand the **Advanced Settings for File Reputation** panel and adjust the following options as needed:

| Option | Description |
|---|---|
| Cloud Domain | The name of the domain to be used for file reputation queries. |

| Option | Description |
|---|---|
| File Reputation Server | Choose either: the host name of the public reputation cloud server, or Private reputation cloud.<br>If you choose Private reputation cloud, provide the following:<br>• **Server** – The host name or IP address of the Cisco AMP Virtual Private Cloud appliance.<br>• **Public Key** – Provide a valid public key for encrypted communications between this appliance and your private cloud appliance. This must be the same key used by the private cloud server: locate the key file on this appliance, and then click **Upload File**.<br>**Note**<br>You must have already downloaded the key file from the server to this appliance. |
| Routing Table | The routing table (associated with an appliance network interface type, either Management or Data) to be used for Advanced Malware Protection services. If the appliance has both the Management interface and one or more Data interfaces enabled, you can select Management or Data. |
| Heartbeat Interval | The frequency, in minutes, with which to ping for retrospective events. |
| Query Timeout | The number of elapsed seconds before the reputation query times out. |
| File Reputation Client ID | The client ID for this appliance on the File Reputation server (read-only). |

**Note**
Do not change any other settings in this section without guidance from Cisco support.

**Step 7** If you will use the cloud service for file analysis, expand the Advanced Settings for File Analysis panel and adjust the following options as needed:

| Option | Description |
|---|---|
| File Analysis Server URL | Choose either: the name (URL) of an external cloud server, or **Private analysis cloud**.<br><br>If specifying an external cloud server, choose the server that is physically nearest to your appliance. Newly available servers will be added to this list periodically using standard update processes.<br><br>Choose Private analysis cloud to use an on-premises Cisco Secure Endpoint Malware Analytics appliance for file analysis, and provide the following:<br><br>• **TG Servers** – Enter the IPv4 address or hostname of the standalone or clustered Cisco Secure Endpoint Malware Analytics appliances. You can add a maximum of seven Cisco Secure Endpoint Malware Analytics appliances.<br><br>**Note**<br>The Serial Number indicates the order in which you add the standalone or clustered Cisco Secure Endpoint Malware Analytics appliances. It does not denote the priority of the appliances.<br><br>**Note**<br>You cannot add standalone and cluster servers in one instance. It must be either standalone or cluster.<br><br>You can add only one standalone server in an instance. If it is a cluster mode, you can add multiple servers upto seven and all the servers must belong to the same cluster. You cannot add multiple clusters.<br><br>• **Certificate Authority** – Choose either **Use Cisco Default Certificate Authority**, or **Use Uploaded Certificate Authority**.<br><br>If you choose Use **Uploaded Certificate Authority**, click **Browse** to upload a valid certificate file for encrypted communications between this appliance and your private cloud appliance. This must be the same certificate used by the private cloud server.<br><br>**Note**<br>If you have configured the Cisco Secure Endpoint Malware Analytics portal on your appliance for file analysis, you can access the Cisco Secure Endpoint Malware Analytics portal (for example, https://panacea.threatgrid.eu) to view and track the files submitted for file analysis. For more information on how to access the Cisco Secure Endpoint Malware Analytics portal, contact Cisco TAC. |
| Proxy Settings | Check **Use File Reputation Proxy** checkbox to use the same File Reputation tunnel proxy that you have already configured, as an upstream proxy for file analysis.<br><br>If you want to configure a different upstream proxy, uncheck the **Use File Reputation Proxy** checkbox and enter the appropriate **Server**, **Port**, **Username**, and **Passphrase** information. |
| File Analysis Client ID | The client ID for this appliance on the File Analysis server (read-only). |

**Step 8** (Optional) Expand the Cache Settings panel, if you want to configure the cache expiry period for File Reputation disposition values.

**Step 9** Expand the Threshold Settings panel, if you want to set the upper limit for the acceptable file analysis score. The score above this threshold indicates that the file is infected. Choose any one of the following options:

- Use value from Cloud Service (95)
- Enter Custom Value – defaults to 95

**Note**
The **Threshold Settings** option are now categorized as **File Analysis Threshold** instead of **Reputation Threshold**.

**Step 10** Submit and commit your changes.

**Step 11** If you are using an on-premises Cisco Secure Endpoint Malware Analytics appliance, activate the account for this appliance on the Cisco Secure Endpoint Malware Analytics appliance.

Complete instructions for activating the "user" account are available in the Cisco Secure Endpoint Malware Analytics documentation.

a) Note the File Analysis Client ID that appears at the bottom of the page section. This identifies the "user" that you will activate.
b) Sign in to the Cisco Secure Endpoint Malware Analytics appliance.
c) Select **Welcome... > Manage Users** and navigate to User Details.
d) Locate the "user" account based on the File Analysis Client ID of your .
e) Activate this "user" account for your appliance.

# Important! Changes Needed in File Analysis Setting

If you plan to use a new public cloud File Analysis service, make sure you read the following instructions to maintain datacenter isolation:

- The existing appliance grouping information is not preserved in the new File Analysis server. You must regroup your appliances on the new File Analysis server.
- Messages that are quarantined to the File Analysis Quarantine are retained until the retention period. After the quarantine retention period, the messages are released from the File Analysis Quarantine, and re-scanned by the AMP engine. The file is then uploaded to the new File Analysis server for analysis but the message is not sent to the File Analysis Quarantine again.

For more details, refer to the Cisco AMP Malware Analytics documentation from https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html.

# (Public Cloud File Analysis Services Only) Configuring Appliance Groups

To allow all content security appliances in your organization to view file analysis result details in the cloud for files sent for analysis from any appliance in your organization, you need to join all appliances to the same appliance group.

**Note** You can configure appliance groups at the machine level. The appliance groups cannot be configured at the cluster level.

### Procedure

**Step 1** Select **Security Services > Anti-Malware and Reputation** .

**Step 2** [Applicable if Smart Licensing is disabled on your email gateway] Enter the group ID manually in the **Appliance ID/Name** field and click **Group Now**.

Or

[Applicable if Smart Licensing is enabled on your email gateway] The system automatically registers the Smart Account ID as group ID and displays it in the **Appliance Group ID/Name** field.

**Notes:**

- An appliance can belong to only one group.
- You can add a machine to a group at any time.
- You can configure appliance groups at the machine and the cluster levels.
- If this is the first appliance being added to the group, provide a useful identifier for the group. This ID is case-sensitive and cannot contain spaces.
- The appliance group ID you provide must be identical on all appliances that will share data about files that are uploaded for analysis. However, the ID is not validated on subsequent appliances in the group.
- If you update the appliance group ID, the change takes effect immediately, and it does not require a Commit.
- You must configure all appliances in a group to use the same File Analysis server in the cloud.
- If Smart Licensing is enabled, the appliances are grouped using the Smart Account ID.

**Step 3** In the Appliance Grouping for File Analysis Cloud Reporting section, enter the File Analysis Cloud Reporting Group ID.

- If this is the first appliance being added to the group, provide a useful identifier for the group.
- This ID is case-sensitive, and cannot contain spaces.
- The ID you provide must be identical on all appliances that will share data about files that are uploaded for analysis. However, the ID is not validated on subsequent group appliances.
- If you enter the Group ID incorrectly or need to change it for any other reason, you must open a case with Cisco TAC.
- This change takes effect immediately; it does not require a Commit.
- All appliances in the group must be configured to use the same File Analysis server in the cloud.
- An appliance can belong to only one group.
- You can add a machine to a group at any time, but you can do it only once.

**Step 4** Click **Add Appliance to Group**.

## Which Appliances Are In the Analysis Group?

**Procedure**

**Step 1** Select **Security Services> Anti-Malware and Reputation** .

**Step 2** In the Appliance Grouping for File Analysis Cloud Reporting section, click **View Appliances in Group**.

**Step 3** To view the **File Analysis Client ID** of a particular appliance, look in the following location:

| Appliance | Location of File Analysis Client ID |
|---|---|
| Email Security appliance | Advanced Settings for File Analysis section on the **Security Services > File Reputation and Analysis** page. |
| Web Security Appliance | Advanced Settings for File Analysis section on the **Security Services > Anti-Malware and Reputation** page. |
| Security Management appliance | At the bottom of the **Management Appliance > Centralized Services > Security Appliances** page. |

# Configuring File Reputation and Analysis Service Action 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 About Advanced Malware Protection Issues

Ensure that the appliance is configured to send you alerts related to Advanced Malware Protection.

You will receive alerts when:

| Alert Description | Type | Severity |
|---|---|---|
| You are setting up a connection to an on-premises (private cloud) Cisco Secure Endpoint Malware Analytics appliance and you need to activate the account as described in Enabling and Configuring File Reputation and Analysis Services. | Anti-Malware | Warning |
| Feature keys expire | (As is standard for all features) | |
| The file reputation or file analysis service is unreachable. | Anti-Malware | Warning |
| Communication with cloud services is established. | Anti-Malware | Info |
| | | Info |
| A file reputation verdict changes. | Anti-Malware | Info |
| File types that can be sent for analysis have changed. You may want to enable upload of new file types. | Anti-Malware | Info |
| Analysis of some file types is temporarily unavailable. | Anti-Malware | Warning |
| Analysis of all supported file types is restored after a temporary outage. | Anti-Malware | Info |
| Invalid File Analysis service key. You need to contact Cisco TAC with the file analysis id details to fix this error. | AMP | Error |

### Related Topics

- Several Alerts About Failure to Connect to File Reputation or File Analysis Servers , on page 299
- Taking Action When File Threat Verdicts Change , on page 298

# 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 topic 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 , on page 296
- File Reputation and File Analysis Report Pages, on page 296
- Viewing File Reputation Filtering Data in Other Reports , on page 297
- About Web Tracking and Advanced Malware Protection Features , on page 297

# 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 | Shows file-based threats that were identified by the file reputation service.<br><br>For files with changed verdicts, see the AMP Verdict updates report. Those verdicts are not reflected in the Advanced Malware Protection report.<br><br>If a file extracted from a compressed or archived file is malicious, only the SHA value of the compressed or archived file is included in the Advanced Malware Protection report.<br><br>The **Incoming Malware Files by Category** section shows the percentage of file SHAs on the blocked list received from the AMP for Endpoints console that are categorised as **Custom Detection**.<br><br>The threat name of file SHA on the blocked list obtained from AMP for Endpoints console is displayed as **Simple Custom Detection** in the Incoming Malware Threat Files section of the report.<br><br>You can click the link in the More Details section of the report to view the file trajectory details about file SHA on the blocked list in the AMP for Endpoints console.<br><br>You can view the **Low Risk** verdict details in the Incoming Files Handed by AMP section of the report. |

| Report | Description |
|---|---|
| Advanced Malware Protection File Analysis | Displays the time and verdict (or interim verdict) for each file sent for analysis. The appliance checks for analysis results every 30 minutes.<br><br>To view more than 1000 File Analysis results, export the data as a .csv file.<br><br>Drill down to view detailed analysis results, including the threat characteristics for each file.<br><br>You can also search for additional information about an SHA, or click the link at the bottom of the file analysis details page to view additional details on the server that analyzed the file.<br><br>**Note**<br>If extracted files from a compressed or an archive file are sent for file analysis, only SHA values of these extracted files are included in the File Analysis report. |
| Advanced Malware Protection Reputation | Because Advanced Malware Protection is focused on targeted and zero-day threats, threat verdicts can change as aggregated data provides more information.<br><br>The AMP Reputation report lists the files processed by this appliance for which the verdict has changed since the message was received. For more information about this situation, see File Threat Verdict Updates , on page 281.<br><br>To view more than 1000 verdict updates, export the data as a .csv file.<br><br>In the case of multiple verdict changes for a single SHA-256, this report shows only the latest verdict, not the verdict history.<br><br>To view all affected messages for a particular SHA-256 within the maximum available time range (regardless of the time range selected for the report) click a SHA-256 link. |

# 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 Message Tracking.

- Web Tracking includes only information about file reputation processing and the original file reputation verdicts returned at the time a transaction message 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.

  No information is provided for clean or unscannable attachments.

  “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 or on-premises File Analysis server. 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.

### What to do next

### Related Topics

File Threat Verdict Updates , on page 281

# Troubleshooting File Reputation and Analysis


- Log Files , on page 299
- Several Alerts About Failure to Connect to File Reputation or File Analysis Servers , on page 299
- API Key Error (On-Premises File Analysis) , on page 300
- Files are Not Uploaded As Expected , on page 300
- File Analysis Details in the Cloud Are Incomplete , on page 300
- Alerts about File Types That Can Be Sent for Analysis , on page 301


## 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.

Information about Advanced Malware Protection including File Analysis is logged in Access Logs or in AMP Engine Logs. For more information, see the topic on monitoring system activity through logs.

In the log message “Response received for file reputation query” possible values for “upload action” are:

- 1: SEND. In this case, you must send the file for File Analysis.
- 2: DON’T SEND. In this case, you do not send the file for File Analysis.
- 3: SEND ONLY METADATA. In this case, you send only the metadata and not the entire file for File Analysis.
- 0: NO ACTION. In this case, no other action is required.

## Several Alerts About Failure to Connect to File Reputation or File Analysis Servers

### Problem

You receive several alerts about failures to connect to the file reputation or analysis services in the cloud. (A single alert may indicate only a transient issue.)

### Solution

- Ensure that you have met the requirements in Requirements for Communication with File Reputation and Analysis Services , on page 286.
- 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.

# API Key Error (On-Premises File Analysis)

**Problem**

You receive an API key alert when attempting to view File Analysis report details, or the is unable to connect to the  AMP Malware Analytics server to upload files for analysis.

**Solution**

This error can occur if you change the hostname of the  AMP Malware Analytics server and you are using a self-signed certificate from the  AMP Malware Analytics server, as well as possibly under other circumstances. To resolve the issue:

- Generate a new certificate from the  AMP Malware Analytics appliance that has the new hostname.
- Upload the new certificate to the .
- Reset the API key on the  AMP Malware Analytics appliance. For instructions, see the online help on the  AMP Malware Analytics appliance.

### Related Topics

- Enabling and Configuring File Reputation and Analysis Services

# Files are Not Uploaded As Expected

**Problem**

Files are not evaluated or analyzed as expected. There is no alert or obvious error.

**Solution**

Consider the following:

- The file may have been sent for analysis by another appliance and thus already be present on the File Analysis server or in the cache of the appliance that is processing the file.
- Check the maximum file size limit configured for the **DVS Engine Object Scanning Limits** on the **Security Services > Anti-Malware and Reputation** page. This limit applies to  Advanced Malware Protection features.

# File Analysis Details in the Cloud Are Incomplete

**Problem**

Complete file analysis results in the public cloud are not available for files uploaded from other Web Security Appliance s in my organization.

**Solution**

Be sure to group all appliances that will share file analysis result data. See (Public Cloud File Analysis Services Only) Configuring Appliance Groups , on page 292. This configuration must be done on each appliance in the group.

# Alerts about File Types That Can Be Sent for Analysis

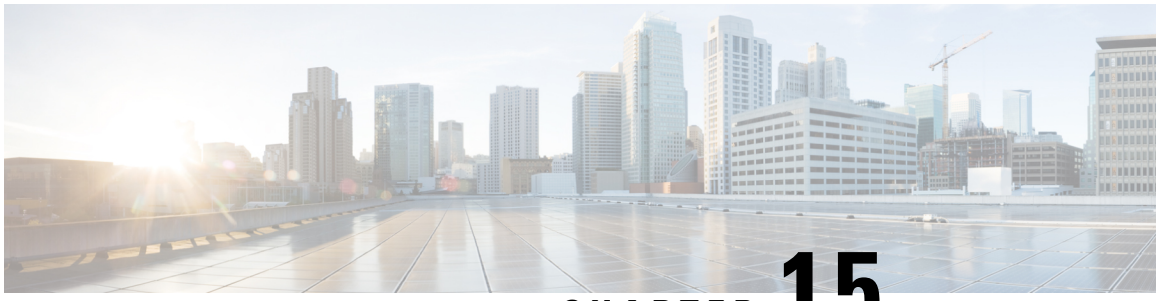
**Problem**

You receive alerts of severity Info about file types that can be sent for file analysis.

**Solution**

This alert is sent when supported file types change, or when the appliance checks to see what file types are supported. This can occur when:

- You or another administrator changes the file types selected for analysis.
- Supported file types change temporarily based on availability in the cloud service. In this case, support for the file types selected on the appliance will be restored as soon as possible. Both processes are dynamic and do not require any action from you.
- The appliance restarts, for example as part of an AsyncOS upgrade.



CHAPTER 15

# Managing Access to Web Applications

This topic contains the following sections:


- Overview of Managing Access to Web Applications, on page 303
- Enabling the AVC Engine, on page 304
- Policy Application Control Settings, on page 305
- Controlling Bandwidth, on page 308
- Controlling Instant Messaging Traffic, on page 311
- Viewing AVC Activity, on page 311


## Overview of Managing Access to Web Applications

The Application Visibility and Control (AVC) engine lets you 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 individually or according to application type. 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
- Specify Range Request settings

To control applications using the AVC engine, perform the following tasks:

| Task | Link to Task |
|---|---|
| Enable the AVC engine | Enabling the AVC Engine, on page 304 |
| Set Controls in an Access Policy Group | Configuring Application Control Settings in an Access Policy Group, on page 308 |
| Limit bandwidth consumed by some application types to control congestion | Controlling Bandwidth, on page 308 |

| Task | Link to Task |
|---|---|
| Allow instant messaging traffic, but disallow file sharing using instant messenger | Controlling Instant Messaging Traffic, on page 311 |

# Enabling the AVC Engine

Enable the AVC engine when you enable the Acceptable Use Controls.



**Note** You can view the AVC engine scanning activity in the Application Visibility report on the Reporting > Application Visibility page.

### Procedure

**Step 1** Choose **Security Services > Acceptable Use Controls**.

**Step 2** Click **Enable** or **Edit Global Settings**, depending on the current status of the Acceptable Use Controls.

**Step 3** Be sure Enable Cisco Web Usage Controls is checked.

**Step 4** In the Acceptable Use Controls Service panel, select **Cisco Web Usage Controls**, and then select **Enable Application Visibility and Control**.

**Step 5** Select the **Default Action for Unreachable Service**: **Monitor** or **Block**.

**Step 6** Submit and Commit Changes.

### What to do next

**Related Topics**

- AVC Engine Updates and Default Actions , on page 304
- User Experience When Requests Are Blocked by the AVC Engine, on page 305

# AVC Engine Updates and Default Actions

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 behaviors change. By updating the AVC engine between AsyncOS version updates, 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; defaults to **Monitor**.

- New applications for an existing application type default to the Application Type's default.

**Note** In the Global Access Policy, you can set the default action for each Application Type, so new applications introduced in an AVC engine update automatically inherit the specified default action. See Configuring Application Control Settings in an Access Policy Group, on page 308.

## User Experience When Requests Are Blocked by the AVC Engine

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; many Websites display dynamic content using JavaScript instead of a static Web page 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.

**Note** When the HTTPS proxy is disabled and Webroot is:

- Enabled - The AVC engine may or may not be launched and return the verdict. The transaction will be processed according to scanner's verdict.
- Disabled - The AVC engine will be launched and return the verdict. The transaction will be processed according to AVC's verdict.

# Policy 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 within an Application Type. |
| Application behaviors | Particular actions or behaviors that users can do within an application that administrators can control. Not all applications include behaviors you can configure. |

You can configure application control settings in Access Policy groups. On the **Web Security Manager** > **Access Policies** page, click the **Applications** link for the policy group you want to configure. When configuring 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<br>**Note**<br>When an application is configured to be blocked under ADC/AVC, every sub-category under the application will also be blocked. A specific sub-category can be blocked using fine and gain control feature, however this feature is limited to certain apps like smugmug, facebook, linkedin, etc. |
| 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. |
| Bandwidth Limit | For certain applications, such as Media and Facebook, you can limit the bandwidth available for Web traffic. You can limit bandwidth for the application itself, and for its users. |

### Related Topics

- Range Request Settings, on page 306
- Rules and Guidelines for Configuring Application Control , on page 307

# Range Request Settings

When HTTP range requests are disabled and a large file is downloaded over multiple streams, the consolidated package is scanned. This disables the performance advantages of download-management utilities and applications that are used to download large objects.

Alternatively, when Range Request Forwarding is enabled (see Configuring Web Proxy Settings, on page 65), you can control how incoming range requests are handled on a per-policy basis. This process is known as “byte serving” and is a means of bandwidth optimization when requesting large files.

However, enabling range request forwarding can interfere with policy-based Application Visibility and Control (AVC) efficiency, and can compromise security. Please exercise caution and enable HTTP Range Request Forwarding only if the advantages outweigh the security implications.



**Note** The Range Request Settings are available only when Range Request Forwarding is enabled, and at least one application is set to Block, Restrict, or Throttle.

| Range Request Settings for Policy |
|---|

| | |
|---|---|
| **Range Request Settings** | • **Do not forward range requests**—The client sends a request for a particular range. But, the Web Security Appliance removes the range header from the request before sending it to the target server. The Web Security Appliance then scans the entire file and sends the range of bytes to the client.<br>**Note**<br>When the client sends the range request for the first time, Web Security Appliance , expecting subsequent range requests from the client, sends the entire file. For any successive request from the same or another client, Web Security Appliance delivers only the partial content to the client.<br>• **Forward range requests**—The client sends a request for a particular range. The Web Security Appliance sends the same request to the target server and receives a partial content which is then returned to the client. The Web Security Appliance scans only the partial content for which the scan results may not be accurate. |
| **Exception list** | You can specify traffic destinations which are exempt from the current forwarding selection. That is, when **Do not forward range requests** is selected, you can specify destinations for which requests are forwarded. Similarly, when **Forward range requests** is selected, you can specify destinations for which requests are not forwarded. |

# Rules and Guidelines for Configuring Application Control

Consider the following rules and guidelines when configuring application control settings:

- The supported Application Types, applications, and application behaviors may change between AsyncOS for Web upgrades, or after AVC engine updates.
- If you enable Safe Search or Site Content Rating, the AVC Engine is tasked with identifying applications for safe browsing. As one of the criteria, the AVC engine will scan the response body to detect a search application. As a result, the appliance will not forward range headers.
- In Application Type listings, the summary for each Application Type lists the final actions for its applications, but does not indicate whether these actions are inherited from the global policy or configured in the current Access Policy. To learn more about the action for a particular application, expand the application type.
- In the Global Access Policy, you can set the default action for each Application Type, so new applications introduced in an AVC engine update automatically inherit the default action.
- You can quickly configure the same action for all applications in an application type by clicking the “edit all” link for the Application Type in Browse view. However, you can only configure the application action, not application behavior actions. To configure application behaviors, you must edit the application individually.
- In Search view, when you sort the table by the action column, the sort order is by the final action. For example, “Use Global (Block)” comes after “Block” in the sort order.
- Decryption may cause some applications to fail unless the root certificate for signing is installed on the client.

### Related Topics

- Configuring Application Control Settings in an Access Policy Group, on page 308
- Configuring Overall Bandwidth Limits, on page 309
- Viewing AVC Activity, on page 311

# Configuring Application Control Settings in an Access Policy Group

### Procedure

**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:

a) Define the default action for each Application Type in the **Default Actions for Application Types** section.

b) You can edit the default actions for each Application Type's individual members, as a group or individually, in the **Edit Applications Settings** section of the page. Editing the default action for individual applications is described in the following steps.

**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:

- **Browse view.** You can browse Application Types. You can use Browse view to configure all 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 its applications; however it 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 by name. You might use Search view when the total list of applications is long and you need to quickly find and configure a particular application.

**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.

### What to do next

### Related Topics

- Controlling Bandwidth, on page 308

# 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 application servers. It does not limit traffic served from the web cache. | Configuring Overall Bandwidth Limits, on page 309 |
| **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, on page 309 |

**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

### Procedure

**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, on page 310 |
| **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, on page 310 |

| Option | Description | Link to task |
|---|---|---|
| **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, on page 311 |

## Configuring the Default Bandwidth Limit for an Application Type

### Procedure

**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.

### Procedure

**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

### Procedure

**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.

### Procedure

**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.

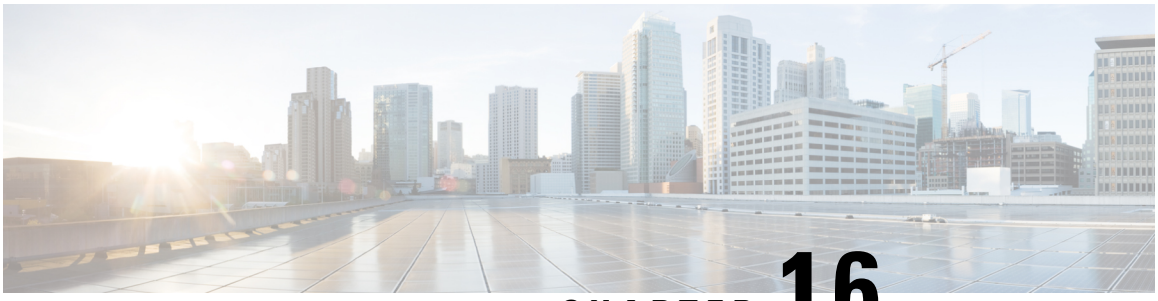
# Viewing AVC Activity

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.

# AVC Information in Access Log File

The access log file records the information returned by the AVC 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 |



CHAPTER 16

# Prevent Loss of Sensitive Data

This topic contains the following sections:


- Overview of Prevent Loss of Sensitive Data, on page 313
- Managing Upload Requests, on page 315
- Managing Upload Requests on an External DLP System, on page 316
- Evaluating Data Security and External DLP Policy Group Membership, on page 316
- Creating Data Security and External DLP Policies, on page 317
- Managing Settings for Upload Requests, on page 319
- Defining External DLP Systems, on page 321
- Controlling Upload Requests Using External DLP Policies, on page 323
- Logging of Data Loss Prevention Scanning , on page 324


## Overview of Prevent Loss of Sensitive Data

The Web Security Appliance secures your data by providing the following capabilities:

| Option | Description |
|---|---|
| Cisco Data Security filters | The Cisco 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 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 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 Data Security policies | Managing Upload Requests, on page 315 |
| Create External DLP policies | Managing Upload Requests on an External DLP System, on page 316 |
| Create Data Security and External DLP policies | Creating Data Security and External DLP Policies, on page 317 |
| Control Upload Requests using Cisco Data Security policies | Managing Settings for Upload Requests, on page 319 |
| Control Upload Requests Using External DLP policies | Controlling Upload Requests Using External DLP Policies, on page 323 |

# 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 Data Security Filters or the external DLP server.

To do this, use the following CLI commands:

- `datasecurityconfig`. Applies to the Cisco 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 Data Security filters or external DLP servers when enabled. However, they can still be bypassed based on a custom URL category.

# User Experience When Requests Are Blocked As Sensitive Data

When the Cisco 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 Web page 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 Data Security filters.

## Procedure

**Create and configure Data Security Policy groups.**

Cisco 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 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.<br>For Cisco 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 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).

### What to do next

**Related Topics**

- Managing Upload Requests on an External DLP System, on page 316
- Managing Settings for Upload Requests, on page 319

# 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:

### Procedure

**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 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.

### What to do next

### Related Topics

- Controlling Upload Requests Using External DLP Policies, on page 323
- Defining External DLP Systems, on page 321

# 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 Identification Profile, fails authentication and is granted guest access, or fails authentication and gets terminated.
- **Authorized users.** If the assigned Identification Profile 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 Identification Profile 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 Identification Profiles 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 Identification Profiles.

### Procedure

**Step 1** Choose **Web Security Manager > Cisco 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 Identification Profile 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 | Choose whether or not to define policy group membership by the protocol used in the client request. Select the protocols to include.<br>"All others" means any protocol not listed above this option.<br>**Note**<br>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. |
| Proxy Ports | 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.<br>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.<br>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.<br>**Note**<br>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. |
| Subnets | Choose whether or not to define policy group membership by subnet or other addresses.<br>You can choose to use the addresses that may be defined with the associated Identification Profile, or you can enter specific addresses here.<br>**Note**<br>If the Identification Profile 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 Identification Profile. Adding addresses in the policy group further narrows down the list of transactions that match this policy group. |
| URL Categories | Choose whether or not to define policy group membership by URL categories. Select the user defined or predefined URL categories.<br>**Note**<br>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. |

| Advanced Option | Description |
|---|---|
| User Agents | Choose whether to define policy group membership by the user agents (client applications such as updaters and Web browsers) used in the client request. You can select some commonly defined user agents, or define your own using regular expressions. Specify whether membership definition includes only the selected user agents, or specifically excludes the selected user agents.<br>**Note**<br>If the Identification Profile associated with this policy group defines Identification Profile membership by this advanced setting, the setting is not configurable at the non-Identification Profile policy group level. |
| User Location | Choose whether or not to define policy group membership by user location, either remote or local.<br>This option only appears when the Secure Mobility is enabled. |

**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.

### What to do next

### Related Topics

- Evaluating Data Security and External DLP Policy Group Membership, on page 316
- Matching Client Requests to Data Security and External DLP Policy Groups, on page 316
- Managing Settings for Upload Requests, on page 319
- Controlling Upload Requests Using External DLP Policies, on page 323

# 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 Polices.

Configure control settings for Data Security Policy groups on the Web Security Manager > Cisco Data Security page.

You can configure the following settings to determine what action to take on upload requests:

| Option | Link |
|---|---|
| **URL Categories** | URL Categories, on page 320 |
| **Web Reputation** | Web Reputation, on page 320 |
| **Content** | Content Blocking, on page 320 |

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 Data Security policies. By definition, all positive scores are monitored.

# Content Blocking

You can use the settings on the Cisco Data Security > 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 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. See SSL Configuration , on page 532for information about specifying the protocols used to secure communications with external DLP servers.

**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

### Procedure

**Step 1** Choose **Network > External DLP Servers**.

**Step 2** Click **Edit Settings**.

| Setting | Description |
|---|---|
| Protocol for External DLP Servers | Choose either:<br>• **ICAP** – DLP client/server ICAP communications are not encrypted.<br>• **Secure ICAP** – DLP client/server ICAP communications are via an encrypted tunnel. Additional related options appear. |

| Setting | Description |
|---|---|
| External DLP Servers | Enter the following information to access an ICAP compliant DLP system:<br>• **Server address** and **Port** – The hostname or IP address and TCP port for accessing the DLP system.<br>• **Reconnection attempts** – The number of times the Web Proxy tries to connect to the DLP system before failing.<br>• **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://<br>• Certificate (optional) – The certificate provided to secure each External DLP Server connection can be Certificate Authority (CA)-signed or self-signed. Obtain the certificate from the specified server, and then upload it to the appliance:<br>  • Browse to and select the certificate file, and then click **Upload File**.<br>  **Note** This single file must contain both the client certificate and private key in unencrypted form.<br>  • **Use this certificate for all DLP servers using Secure ICAP** – Check this box to use the same certificate for all External DLP Servers you define here. Leave the option unchecked to enter a different certificate for each server.<br>• Start Test – You can test the connection between the Web Security Appliance and the defined external DLP server(s) by clicking **Start Test**. |
| Load Balancing | 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:<br>• **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.<br>• **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.<br>• **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.<br>• **Round robin.** The Web Proxy cycles upload requests equally among all DLP servers in the listed order. |
| Service Request Timeout | 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.<br>Default is 60 seconds. |

| Setting | Description |
|---|---|
| Maximum Simultaneous Connections | 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.<br>Default is 25. |
| Failure Handling | Choose whether upload requests are blocked or allowed (passed to Access Policies for evaluation) when the DLP server fails to provide a timely response.<br>Default is allow ("Permit all data transfers to proceed without scanning"). |
| Trusted Root Certificate | Browse to and select the trusted-root certificate for the certificate(s) provided with the External DLP Servers, and then click Upload File. See Certificate Management, on page 533 for additional information. |
| Invalid Certificate Options | Specify how various invalid certificates are handled: **Drop** or **Monitor**. |
| Server Certificates | This section displays all DLP server certificates currently available on the appliance. |

**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** 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).

### Procedure

**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 except to specified custom and external URL categories.** Upload requests that fall in specific custom URL categories are excluded from DLP scanning policies. Click **Edit custom categories list** to select the URL categories to scan.

**Step 5** Submit and Commit Changes.

# Logging of Data Loss Prevention Scanning

The access logs indicate whether or not an upload request was scanned by either the Cisco Data Security filters or an external DLP server. The access log entries include a field for the Cisco 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 Data Security and External DLP Policies:

- **Data Security Logs.** Records client history for upload requests that are evaluated by the Cisco Data Security filters.
- **Data Security Module Logs.** Records messages related to the Cisco 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:

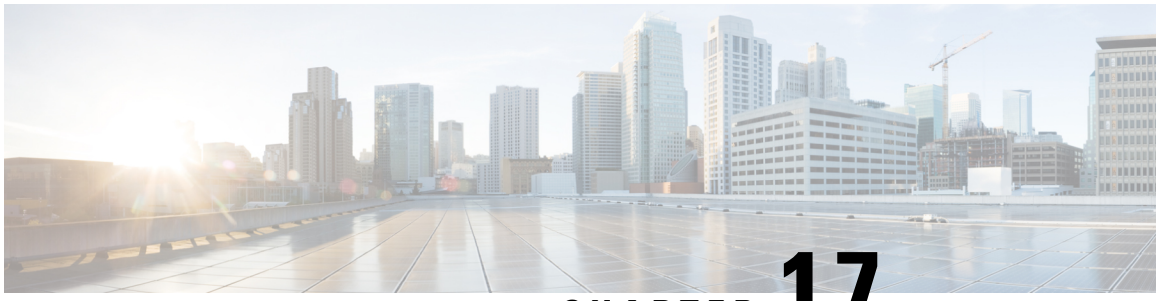
```
Mon Mar 30 03:02:13 2009 Info: 303 10.1.1.1 - -
<<bar,text/plain,5120><foo,text/plain,5120>>
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting ns server.com nc
```

| 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<br>**Note**<br>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 Data Security policy and action |

| Field Value | Description |
|---|---|
| `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.



CHAPTER 17

# Notify End-Users of Proxy Actions

This topic contains the following sections:


- End-User Notifications Overview, on page 327
- Configuring General Settings for Notification Pages, on page 328
- End-User Acknowledgment Page, on page 328
- End-User Notification Pages , on page 332
- Configuring the End-User URL Filtering Warning Page, on page 335
- Configuring FTP Notification Messages, on page 336
- Custom Messages on Notification Pages, on page 337
- Editing Notification Page HTML Files Directly , on page 338
- Notification Page Types, on page 342


## End-User Notifications Overview

You can configure the following types of notifications for end users:

| Option | Description | Further information |
|---|---|---|
| End-user acknowledgement page | Informs end users that their web activity is being filtered and monitored. An end-user acknowledgment page is displayed when a user first accesses a browser after a certain period of time. | End-User Acknowledgment Page, on page 328 |
| End-user notification pages | Page shown to end users when access to a particular page is blocked, specific to the reason for blocking it. | End-User Notification Pages , on page 332 |
| End-user URL filtering warning page | Warns end users that a site they are accessing does not meet your organization's acceptable use policies, and allows them to continue if they choose. | Configuring the End-User URL Filtering Warning Page, on page 335 |
| FTP notification messages | Gives end users the reason a native FTP transaction was blocked. | Configuring FTP Notification Messages, on page 336. |

| Option | Description | Further information |
|---|---|---|
| Time and Volume Quotas Expiry Warning Page | Notifies end users when their access is blocked because they have reached the configured data volume or time limit. | Configure these settings on the Security Services > End User Notification page, Time and Volume Quotas Expiry Warning Page section.<br>See also Time Ranges and Quotas, on page 233. |

# Configuring General Settings for Notification Pages

Specify display languages and logo for notification pages. Restrictions are described in this procedure.

### Procedure

**Step 1** Select **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 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).
- The FTP language applies to all FTP notification messages.

**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.

This setting applies to all HTTP notification pages served over IPv4. AsyncOS does not support images over IPv6.

**Step 5** Submit and Commit Changes.

### What to do next

### Related Topics

- Caveats for URLs and Logos in Notification Pages , on page 337

# 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.


- Access HTTPS and FTP Sites with the End-User Acknowledgment Page, on page 329
- About the End-user Acknowledgment Page, on page 329
- Configuring the End-User Acknowledgment Page, on page 330


# 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 and Identity policy that exempts users from the end-user acknowledgment page for this custom URL category.

# About the End-user Acknowledgment Page

- When a user is tracked by IP address, the appliance uses the shortest value for maximum time interval and maximum IP address idle timeout to determine when to display the end-user acknowledgment page again.
- When a user is tracked using a session cookie, the Web Proxy displays the end-user acknowledgment page again if the user closes and then reopens their web browser or opens a second web browser application.
- Using a session cookie to track users when the client accesses HTTPS sites or FTP servers using FTP over HTTP does not work.
- When the appliance is deployed in explicit forward mode and a user goes to an HTTPS site, the end-user acknowledgment page includes only the domain name in the link that redirects the user to the originally requested URL. If the originally requested URL contains text after the domain name, that text is truncated.
- When the end-user acknowledgment page is displayed to a user, the access log entry for that transaction shows OTHER as the ACL decision tag. This is because the originally requested URL was blocked, and instead the user was shown the end-user acknowledgment page.

# Configuring the End-User Acknowledgment Page

### Before you begin

- To configure the display language and customize the displayed logo, see Configuring General Settings for Notification Pages, on page 328.
- If you will customize the message shown to end users, see Custom Messages on Notification Pages, on page 337. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 338.

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`.

### Procedure

**Step 1** Choose **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** Enter options:

| Setting | Description |
|---|---|
| **Time Between Acknowledgements** | 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).<br>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. |
| **Inactivity Timeout** | 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 to have agreed to the acceptable use policy. You can specify any value from 30 to 2678400 seconds (one month). Default is four hours (14400 seconds). |

| Setting | Description |
|---|---|
| **Surrogate Type** | Determines which method the Web Proxy uses to track the user:<br>• **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.<br>**Note**<br>When IP address is configured and the user is authenticated, the Web Proxy tracks users by username instead of IP address.<br>• **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.<br>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.<br>**Note**<br>Using a session cookie to track users when the client accesses HTTPS sites or FTP servers using FTP over HTTP is not supported. |
| **Custom message** | Customize the text that appears on every end-user acknowledgment page. You can include some simple HTML tags to format the text.<br>**Note**<br>You can only include a custom message when you configure the end-user acknowledgment page in the web interface, versus the CLI.<br>See also Custom Messages on Notification Pages, on page 337. |

**Step 5** (Optional) Click **Preview Acknowledgment Page Customization** to view the current end-user acknowledgment page in a separate browser window.

**Note**
If the notification HTML files have been edited, this preview functionality is not available.

**Step 6** Submit and Commit Changes.

# End-User Notification Pages

When a policy blocks a user from a website, you can configure the appliance to notify the user why it blocked the URL request. There are several ways to achieve this:

| To | See |
|---|---|
| Display predefined, customizable pages that are hosted on the Web Security Appliance . | Configuring On-Box End-User Notification Pages, on page 332 |
| Redirect the user to HTTP end-user notification pages at a specific URL. | Off-Box End-User Notification Pages , on page 333 |

# Configuring On-Box End-User Notification Pages

### Before you begin

- To configure the display language and customize the displayed logo, see Configuring General Settings for Notification Pages, on page 328.
- If you will customize the message displayed using on-box notifications, review the topics under Custom Messages on Notification Pages, on page 337. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 338.

On-box pages are predefined, customizable notification pages residing on the appliance.

### Procedure

**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.<br>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. |

| Setting | Description |
|---|---|
| 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.<br>**Note**<br>• You must enable SensorBase Network Participation. See Enabling Participation in The Cisco SensorBase Network for more information.<br>• You must have a valid Cisco account linked to the serial number/s of your appliance/s.<br>• Reporting of misclassified URLs does not work on virtual Web Security Appliance . |

**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 notification HTML files have been edited, this preview functionality is not available.

**Step 6** Submit and Commit Changes.

# Off-Box End-User Notification Pages

The Web Proxy can be configured to redirect all HTTP end-user notification pages to a specific URL that you specify.


- Displaying the Correct Off-Box Page Based on the Reason for Blocking Access , on page 333
- URL Criteria for Off-Box Notification Pages , on page 333
- Off-Box End-User Notification Page Parameters, on page 334
- Redirecting End-User Notification Pages to a Custom URL (Off-Box) , on page 335


## Displaying the Correct Off-Box Page Based on the Reason for Blocking Access

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 Off-Box End-User Notification Page Parameters, on page 334.

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.

## URL Criteria for Off-Box Notification Pages

- You can use any HTTP or HTTPS URL.
- The URL may specify a specific port number.
- The URL may not have any arguments after the question mark.
- The URL must contain a well-formed hostname.

For example, if you have the following URL entered in the Redirect to Custom URL field:

```
http://www.example.com/eun.policy.html
```

And you have the following access log entry:

```
1182468145.492 1 172.17.0.8 TCP_DENIED/403 3146 GET http://www.espn.com/index.html HTTP/1.1
 - NONE/- - BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
<IW_sprt,-,-,-,-,-,-,-,-,-,-,-,-,-,IW_sprt,-> -
```

Then AsyncOS creates the following redirected URL:

```
http://www.example.com/eun.policy.html?Time=21/Jun/
2007:23:22:25%20%2B0000&ID=0000000004&Client_IP=172.17.0.8&User=-
&Site=www.espn.com&URI=index.html&Status_Code=403&Decision_Tag=
BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
&URL_Cat=Sports%20and%20Recreation&WBRS=-&DVS_Verdict=-&
DVS_ThreatName=-&Reauth_URL=-
```

## Off-Box 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.<br>**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. |

| Parameter Name | Description |
|---|---|
| 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.<br>To use this parameter, make sure the CGI script performs the following steps:<br>1. Get the value of `Reauth_Url` parameter.<br>2. URL-decode the value.<br>3. Base64 decode the value and get the actual re-authentication URL.<br>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 (Off-Box)

### Procedure

**Step 1** **Security Services > End-User Notification**.
**Step 2** Click **Edit Settings**.
**Step 3** In the **End-User Notification Pages** section, 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.

# Configuring the End-User URL Filtering Warning Page

### Before you begin

- If you will customize the message displayed using on-box notifications, review the topics under Custom Messages on Notification Pages, on page 337. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 338.

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.

### Procedure

**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.

**Note**
If the notification HTML files have been edited, this preview functionality is not available.

**Step 7** Submit and Commit Changes.

# Configuring FTP Notification Messages

### Before you begin

If you will customize the message displayed using on-box notifications, review the topics under Custom Messages on Notification Pages, on page 337. If you require more customization than the Custom Message box allows, see Editing Notification Page HTML Files Directly , on page 338.

The FTP Proxy displays a predefined, customizable 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. The notification is specific to the reason the connection was blocked.

### Procedure

**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 Messages on Notification Pages

The following sections apply to text entered into the "Custom Message" box for any notification type configured on the Edit End User Notification page.


- Supported HTML Tags in Custom Messages on Notification Pages, on page 337
- Caveats for URLs and Logos in Notification Pages , on page 337


## Supported HTML Tags in Custom Messages on Notification Pages

You can use HTML tags to format the text in any notification on the Edit End User Notification page that offers a "Custom Message" box. Tags must be in lower case and follow standard HTML syntax (closing tags, etc.)

You can use the following HTML tags.

- <a></a>
- 
- 
- <big></big>
- <br>
- <code></code>
- 
- 
- <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.
```

**Note** If you need greater flexibility or wish to add JavaScript to your notification pages, you must edit the HTML notification files directly. JavaScript entered into the Custom Message box for notifications in the web user interface will be stripped out. See Editing Notification Page HTML Files Directly , on page 338.

## Caveats for URLs and Logos in Notification Pages

This section applies if you will make any of the following customizations:

- Enter text into the "Custom Message" box for any notification on the Edit End User Notification page

- Directly edit HTML files for on-box notifications
- Use a custom logo

All combinations of URL paths and domain names in embedded links within custom text, and the custom logo, are exempted from the following for on-box notifications:

- 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 you to create a more sophisticated page with embedded content so long as the embedded content is relative to the initial URL. However, you should also take care when deciding which paths to include as links and custom logos.

# Editing Notification Page HTML Files Directly

Each notification page is stored on the Web Security Appliance as an HTML file. If you require more customization than the “Custom Message” box in the web-based interface allows, you can directly edit these HTML files. For example, you can include standard JavaScript or edit the overall look and feel of each page.

Information in the following sections applies to any type of end-user notification HTML file on the appliance, including End-User Acknowledgment pages.

- Requirements for Editing Notification HTML Files Directly , on page 338
- Editing Notification Page HTML Files Directly , on page 338
- Using Variables in Notification HTML Files , on page 340
- Variables for Customizing Notification HTML Files , on page 340

## Requirements for Editing Notification HTML Files Directly

- Each notification page file must be a valid HTML file. For a list of HTML tags you can include, see Supported HTML Tags in Custom Messages on Notification Pages, on page 337.

- The customized notification page file names must exactly match the file names shipped with the Web Security Appliance .

  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.
- 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.
- Test your HTML files in supported client browsers to ensure that they behave as expected, especially if they include JavaScript.
- For your customized pages to take effect, you must enable the customized files using the `advancedproxyconfig > EUN > Refresh EUN Pages` CLI command.

# Editing Notification HTML Files Directly

### Before you begin

- Understand the requirements in Requirements for Editing Notification HTML Files Directly , on page 338.
- See Variables for Customizing Notification HTML Files , on page 340 and Using Variables in Notification HTML Files , on page 340.

### Procedure

**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 notification pages you want to edit.

**Step 4** On your local machine, use a text or HTML editor to edit the HTML files.

**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.

**Step 9** If the custom end-user notification pages option is currently enabled when you update the HTML files, 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 10** Commit your change.

**Step 11** Close the SSH client.

# Using Variables in Notification HTML Files

When editing notification HTML files, 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 |
|---|---|
| %?*V* | This conditional variable evaluates to TRUE if the output of variable %*V* is not empty. |
| %!*V* | Represents the following condition:<br>`else`<br>Use this with the %?*V* conditional variable. |
| %#*V* | Represents the following condition:<br>`endif`<br>Use this with the %?*V* 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 Variables for Customizing Notification HTML Files , on page 340 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.

# Variables for Customizing Notification HTML Files

You can use variables in the notification 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 Using Variables in Notification HTML Files , on page 340.

| 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 |

| Variable | Description | Always Evaluates to TRUE if Used as Conditional Variable |
|---|---|---|
| %c | Error page contact person | Yes |
| %C | Entire Set-Cookie: header line, or empty string | No |
| %d | Client IP address | Yes |
| %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 |

| Variable | Description | Always Evaluates to TRUE if Used as Conditional Variable |
|---|---|---|
| %Q | Policy group name for non-Identity polices | 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 |
| %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 |

# 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 Variables for Customizing Notification HTML Files , on page 340.

The table describes the different notification pages users might encounter.

| File Name and Notification Title | Notification Description | Notification Text |
|---|---|---|
| ERR_ACCEPTED<br>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<br>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<br>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.<br>Click here to accept this statement and access the Internet. |
| ERR_AVC<br>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<br>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.<br>If you are using a standard browser, please retry the request. |
| ERR_BLOCK_DEST<br>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<br>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 "<*malware name* >".<br>Please contact <*contact name* > <*email address* > and provide the codes shown below.<br>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<br>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 "<*browser type* >" is not permitted due to potential security risks. |
| ERR_CERT_INVALID<br>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 <*hostname* > provided an invalid certificate. |
| ERR_CONTINUE_ UNACKNOWLEDGED<br>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 <*URL category* >. 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.<br>Click here to accept this statement and access the Internet. |

| File Name and Notification Title | Notification Description | Notification Text |
|---|---|---|
| ERR_DNS_FAIL<br>DNS Failure | Error page that is displayed when the requested URL contains an invalid domain name. | The hostname resolution (DNS lookup) for this hostname <*hostname* > has failed. The Internet address may be misspelled or obsolete, the host <*hostname* > may be temporarily unavailable, or the DNS server may be unresponsive.<br>Please check the spelling of the Internet address entered. If it is correct, try this request later. |
| ERR_EXPECTATION_FAILED<br>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 <*URL* >. A non-standard browser may have generated an invalid HTTP request.<br>If using a standard browser, please retry the request. |
| ERR_FILE_SIZE<br>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<br>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<br>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.<br>Please retry the request later. |
| ERR_FOUND<br>Found | Internal redirection page for some errors. | The page <*URL* > is being redirected to <*redirected URL* >. |
| ERR_FTP_ABORTED<br>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.<br>Please retry the request later. |

| File Name and Notification Title | Notification Description | Notification Text |
|---|---|---|
| ERR_FTP_AUTH_REQUIRED<br>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 passphrase must be entered when prompted.<br>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<br>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.<br>Please check the spelling of the address entered. If it is correct, try this request later. |
| ERR_FTP_FORBIDDEN<br>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<br>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_ERR<br>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.<br>Please confirm that this is a valid address. If it is correct, try this request later. |
| ERR_FTP_SERVICE_UNAVAIL<br>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.<br>Please confirm that this is a valid address. If it is correct, try this request later. |

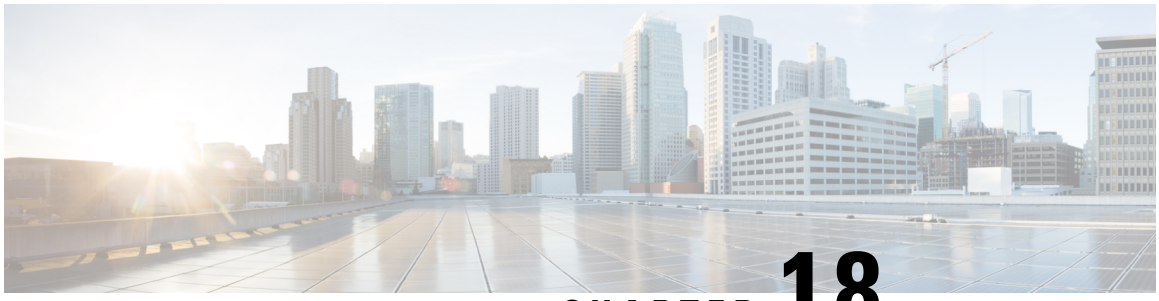
| File Name and Notification Title | Notification Description | Notification Text |
|---|---|---|
| ERR_GATEWAY_TIMEOUT<br>Gateway Timeout | Error page that is displayed when the requested server has not responded in a timely manner. | The system cannot communicate with the external server <*hostname* >. The Internet server may be busy, may be permanently down, or may be unreachable because of network problems.<br>Please check the spelling of the Internet address entered. If it is correct, try this request later. |
| ERR_IDS_ACCESS_FORBIDDEN<br>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:<br><*file details* > |
| ERR_INTERNAL_ERROR<br>Internal Error | Error page that is displayed when there is an internal error. | Internal system error when processing the request for the page <*URL* >.<br>Please retry this request.<br>If this condition persists, please contact <*contact name* > <*email address* > and provide the code shown below. |
| ERR_MALWARE_SPECIFIC<br>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.<br>Malware <*malware name* > in the category <*malware category* > has been found on this site. |
| ERR_MALWARE_SPECIFIC_OUTGOING<br>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.<br>Malware Name: <*malware name* ><br>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<br>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.<br>The server address <*hostname* > may be invalid, or you may need to specify a port number to access this server. |
| ERR_POLICY<br>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<br>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<br>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 passphrase must be entered when prompted. |
| ERR_PROXY_PREVENT_ MULTIPLE_LOGIN<br>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.<br>If you want to login as a different user, click on the button below and enter a different a user name and passphrase. |
| ERR_PROXY_REDIRECT<br>Redirect | Redirection page. | This request is being redirected. If this page does not automatically redirect, click here to proceed. |

| File Name and Notification Title | Notification Description | Notification Text |
|---|---|---|
| ERR_PROXY_UNACKNOWLEDGED<br>Policy Acknowledgment | End-user acknowledgment page.<br>For more information, see End-User Notification Pages , on page 332. | Please acknowledge the following statements before accessing the Internet.<br>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 polices on Internet access.<br>Click here to accept this statement and access the Internet. |
| ERR_PROXY_UNLICENSED<br>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.<br>Please contact <*contact name*> <*email address*> and provide the code shown below.<br>**Note**<br>To access the management interface of the security device, enter the configured IP address with port. |
| ERR_RANGE_NOT_SATISFIABLE<br>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.<br>If you are using a standard browser, please retry the request. |
| ERR_REDIRECT_PERMANENT<br>Redirect Permanent | Internal redirection page. | The page <*URL*> is being redirected to <*redirected URL*>. |
| ERR_REDIRECT_REPEAT_REQUEST<br>Redirect | Internal redirection page. | Please repeat your request. |

| File Name and Notification Title | Notification Description | Notification Text |
|---|---|---|
| ERR_SAAS_AUTHENTICATION<br>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<br>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 passphrase for a user that is authorized to access this application. |
| ERR_SAML_PROCESSING<br>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<br>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<br>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.<br>Please contact <*contact name* > <*email address* > and provide the code shown below. |
| ERR_WBRS<br>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.<br>Threat Type: %o<br>Threat Reason: %O |

| File Name and Notification Title | Notification Description | Notification Text |
|---|---|---|
| ERR_WEBCAT<br>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_ REQUIRED<br>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 passphrase must be entered when prompted. |



CHAPTER 18

# Generate Reports to Monitor End-user Activity

This topic contains the following sections:


- Overview of Reporting , on page 353
- Using the Reporting Pages, on page 355
- Using the Interactive Report Pages on the New Web Interface, on page 360
- Enabling Reporting, on page 360
- Scheduling Reports, on page 361
- Generating Reports On Demand, on page 363
- Archived Reports, on page 363
- Troubleshooting L4 Traffic Monitor Reports , on page 364


## Overview of Reporting

The Web Security Appliance  generates high-level reports, allowing you to understand what is happening on the network and also allowing 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, on page 359


## 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.

**Procedure**

**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:

- My Dashboard (the reporting “homepage”; can also be accessed by clicking the Home icon in the left edge of the menu bar)
- Overview
- Users
- User Count
- Web Sites
- URL Categories
- Application Visibility
- Anti-Malware
- Advanced Malware Protection
- File Analysis
- AMP Verdict Updates
- Client Malware Risk
- Web Reputation Filters
- L4 Traffic Monitor
- SOCKS Proxy
- Reports by User Location
- Web Tracking
- System Capacity
- System Status
- Scheduled Reports
- Archived Reports

# Using the Reporting Pages

The various report pages provide an overview of system activity and support multiple options for viewing the system data. You can also search each page for Website and client-specific data.

You can perform the following tasks on most report pages:

| Option | Link to Task |
|---|---|
| **Change the time range displayed by a report** | Changing the Time Range, on page 355 |
| **Search for specific clients and domains** | Searching Data, on page 356 |
| **Choose which data to display in charts** | Choosing Which Data to Chart , on page 357 |
| **Export reports to external files** | Printing and Exporting Reports from Report Pages, on page 359 |

## 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 complete minutes plus up to 5 additional minutes. |
| Day | One-hour intervals for the last 24 hours and including the current partial hour. |
| Week | On- 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 time zone defined on the Web Security Appliance . |
| Custom Range | The custom time range you defined.<br>When you choose Custom Range, a dialog box appears to let you enter start and end times. |

**Note** All reports display date and time information based on the system's configured time zone, shown as a Greenwich Mean Time (GMT) offset. However, data exports display the time in GMT only to accommodate multiple systems in multiple time zones around the world.

# Choosing a Time Range for Reports

Most predefined report pages allow you to choose a Time Range for the data to include. The time range that you select is used for all of the report pages until you select a different value in the Time Range menu.

Available Time Range options differ by appliance and differ for Email and Web reporting on the Security Management appliance:

**Note** Time ranges on report pages are displayed as a Greenwich Mean Time (GMT) offset. For example, Pacific time is GMT + 7 hours (GMT + 07:00).

**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 you can use 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.

### Procedure

**Step 1** Click the **Chart Options** link below a chart.

**Step 2** Choose the data to display.

**Step 3** Click **Done**.

# 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:<br>• Modules That Cannot Be Added to Custom Reports , on page 358.<br>• Creating Your Custom Report Page , on page 358 |
| View your custom report page | 1. Choose **Monitor > Email or Web > Reporting > Reporting > My Reports.**<br>2. Select the time range to viewThe time range selected applies to all reports, including all modules on the My Reports page.<br>Newly-added modules appear at the top of the relevant section. |
| 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 | Choose **Reporting > Archived Reports** and click **Generate Report Now**. |
| Periodically generate a PDF or CSV version of your custom report | Choose **Reporting > Scheduled Reports.** |

## Modules That Cannot Be Added to Custom Reports

- Search results , including Web Tracking search results

## Creating Your Custom Report Page

### Before you begin

- Ensure that the modules that you want to add can be added. See Modules That Cannot Be Added to Custom Reports , on page 358.
- Delete any default modules that you do not need by clicking the [**X**] in the top right corner of those module.

### Procedure

**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 under the that has the module 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.

# 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, although 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-formatted PDF version of any report page 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 the time zone 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 07:00 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. |
| `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.

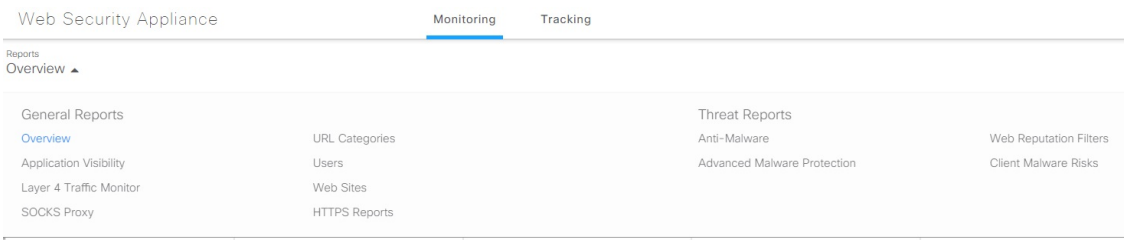
- If you export localized CSV data, the headings may not be rendered properly in some browsers. This occurs because some browsers may not use the proper character set for the localized text. To work around this problem, you can save the file to your local machine, and open the file in any Web browser using **File > Open**. When you open the file, select the character set to display the localized text.

# Using the Interactive Report Pages on the New Web Interface

You can view the reports for the Web Security Appliance using the **Reports** drop-down as shown in the following figure:

**Note** The Overview report page is the landing page (the page displayed after login). Reloading the new web interface from any reporting or tracking page loads the default landing page (Overview report page).

***Figure 10: Reports Drop-down***




The web reports as categorized as: **General Reports** and **Threat Reports**.

To access the new web interface, see Secure Appliance Reports on the New Web Interface.

### Related Topics

- (Web Reports Only) Choosing Which Data to Chart, on page 404

# Enabling Reporting

If your organization has multiple Web Security Appliance s and uses a Cisco Content Security Management Appliance to manage and view aggregated report data, you must enable centralized reporting on each Web Security Appliance .

You can choose the type of reporting based on the appliance setup. You can choose to retain all reports locally. If your organization has multiple Web Security Appliance s and uses a Cisco Content Security Management Appliance, you can choose centralized reporting to manage and view aggregated report data. If you choose Centralized Reporting or local reporting , you have to apply these selections on each Web Security Appliance .

**Procedure**

**Step 1** Choose **Security Services** > **Reporting**, and click **Edit Settings**.

a) Select **Local Reporting** to enable reporting on the appliance. The reports will be accessible after logging in to the appliance portal.

b) Select **Centralized Reporting** to enable reporting through Cisco Content Security Management Appliance.

The Web Security Appliance only stores all its collected data for local reporting. If Centralized Reporting is enabled on the appliance, then the Web Security Appliance retains *only* System Capacity and System Status data, and those are the only reports available on the Web Security Appliance locally.

See the topic "Using Centralized Web Reporting and Tracking" in your Cisco Content Security Management Appliance user guide for information about configuring this feature on the management appliance.

**Step 2** **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
- Advanced Malware Protection
- Advanced Malware Protection Verdict Updates
- Client Malware Risk
- Web Reputation Filters
- L4 Traffic Monitor
- SOCKS Proxy
- Reports by User Location
- System Capacity
- My Dashboard

# Adding a Scheduled Report

**Procedure**

**Step 1** Choose **Reporting > Scheduled Reports** and click **Add Scheduled Report**.

**Step 2** Choose a report **Type**.

**Step 3** Enter a descriptive **Title** for the report.

Avoid creating multiple reports with the same name.

**Step 4** Choose a time range for the data included in the report.

**Step 5** Select 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 to** field, enter the email address(es) to which the generated report is to be sent.

If you do not specify an email address, the report is simply archived.

**Step 9** Choose a **Report Language** for the data.

**Step 10** Submit and Commit Changes.

# Editing Scheduled Reports

**Procedure**

**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

**Procedure**

**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

**Procedure**

**Step 1** Choose **Reporting** > **Archived Reports**.

**Step 2** Click **Generate Report Now.**

**Step 3** Choose a report **Type**.

**Step 4** Enter a descriptive **Title** for the report.

Avoid creating multiple reports with the same name.

**Step 5** Choose a time range for the data included in the report.

**Step 6** Select 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 7** 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 8** Select one of the **Delivery Options**:

- **Archive** the report (the report will appear on the Archived Reports page).
- **Email now to recipients**; provide one or more email addresses.

**Step 9** Choose a **Report Language** for the data.

**Step 10** Click **Deliver this Report** to generate the report.

**Step 11** Commit Changes.

# Archived Reports

The **Reporting** > **Archived Reports** page lists available archived reports. Each name in the Report Title column provides a link to a view of that report. The **Show** menu filters the types of reports that are listed. The column headings can be clicked to sort the data in each column.

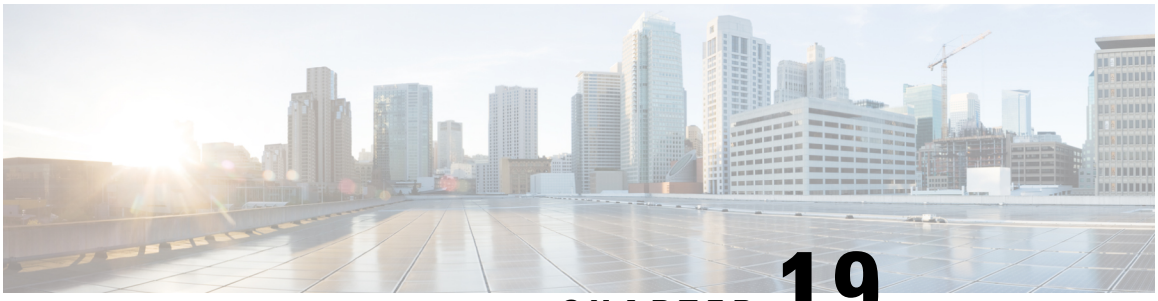
The appliance stores up to 12 instances of each scheduled report (up to a total of 1000 reports). Archived reports are stored in the `/periodic_reports` directory on the appliance. Archived reports are deleted automatically. As new reports are added, older reports are removed to keep the number at 1000. The limit of 12 instances applies to each scheduled report with the same name and time range.

# Troubleshooting L4 Traffic Monitor Reports

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 the client IP address in reports. If the Web Proxy is configured as a transparent proxy, enable IP spoofing to correctly record and display the client IP addresses. To do this, see the IronPort AsyncOS for Web User Guide.

### Related Topics

- Client Malware Risk Page, on page 371
- Searching for Transactions Processed by the L4 Traffic Monitor , on page 377



CHAPTER 19

# Secure Appliance Reports

This topic contains the following sections:


- Overview Page, on page 365
- Users Page, on page 367
- User Count Page, on page 368
- Web Sites Page, on page 368
- URL Categories Page, on page 369
- Application Visibility Page, on page 370
- Anti-Malware Page, on page 370
- Advanced Malware Protection Page, on page 371
- File Analysis Page, on page 371
- AMP Verdict Updates Page , on page 371
- Client Malware Risk Page, on page 371
- Web Reputation Filters Page, on page 372
- L4 Traffic Monitor Page, on page 372
- SOCKS Proxy Page , on page 373
- Reports by User Location Page, on page 373
- Web Tracking Page , on page 374
- System Capacity Page, on page 378
- System Status Page, on page 378


# 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 .

***Table 7: System Overview***

| Section | Description |
|---|---|
| Web Proxy Traffic Characteristics | `Listing of Average transactions per second in past minute`, `Average bandwidth (bps) in past minute`, `Average response time (ms) in past minute`, and `Total current connections`. |

| Section | Description |
|---|---|
| System Resource Utilization | Listing of current `Overall CPU Load`, `RAM` and `Reporting / logging disk` usage. Click **System Status Details** to switch to the System Status page (see System Status Page on the New Web Interface, on page 414 for details).<br>**Note**<br>The CPU utilization value shown on this page and the CPU value shown on the System Status page may differ slightly because they are read separately, at differing moments. |

***Table 8: Time Range-based Categories and Summaries***

| Section | Description |
|---|---|
| Time Range: Choose a time range for the data displayed in the following sections. Options are Hour, Day, Week, 30 Days, Yesterday, or a Custom Range. | |
| 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). |
| 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.<br>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: Total Transactions | Displays the top 10 URL categories that have been blocked. |
| Top Application Types: Total Transactions | |
| Top Malware Categories: Monitored or Blocked | 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. |
| Web Traffic Tap Status | Displays the untapped and tapped traffic transactions in a graph format. |
| Web Traffic Tap Summary | Displays the summary of the tapped and untapped traffic transactions along with the total traffic transactions. |
| Tapped HTTP/HTTPS Traffic | Displays the tapped HTTP and HTTPS traffic transactions in a graph format. |
| Tapped Traffic Summary | Displays the summary of HTTP and HTTPS traffic transactions along with the total HTTP/HTTPS traffic transactions. |

| Section | Description |
|---|---|
| EUP Transactions | Displays encapsulated URL transactions. These are transactions that were performed through websites like *translate.google.com*. |
| EUP Transaction Summary | Displays the summary of encapsulated URL transactions. |
| EUP Suspect Transactions | Displays the encapsulated URL transactions that were found to be suspect. |
| EUP Suspect Transaction Summary | Displays the summary of encapsulated URL transactions that were found to be suspect. |

# 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. |

| Section | Description |
|---|---|
| Domains Matched | Displays information about a specific Domain or IP address that this user has accessed.<br>**Note**<br>If you export this Domains data to a CSV file, be aware that only the first 300,000 entries are exported to the file. |
| Applications Matched | |
| 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. |

# User Count Page

The **Reporting** > **User Count** page displays information about the total number of authenticated and unauthenticated users of the appliance. The page lists the unique user count for the last 30 days, 90 days, and 180 days.



**Note** System computes the total user count of authenticted and unauthenticated users once a day.

For example, if you view the user count report on May 22, 23:59, at the latest, the system will display the total user count till May 22, 00:00.

# 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.<br>**Note**<br>If you export this Domains data to a CSV file, be aware that only the first 300,000 entries are exported to the file. |

# 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.<br>If the percentage of uncategorized URLs is higher than 15-20%, consider the following options:<br>• For specific localized URLs, you can create custom URL categories and apply them to specific users or group policies.<br>• You can report uncategorized and misclassified and URLs to the Cisco for evaluation and database update.<br>• 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

| 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. |
| 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 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

**Procedure**

**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

**Procedure**

**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 Filtering and File Analysis, on page 281.

# File Analysis Page

See File Reputation and File Analysis Reporting and Tracking , on page 295.

# AMP Verdict Updates Page

See File Reputation Filtering and File Analysis, on page 281.

See .

# 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.

### Procedure

**Step 1** Choose **Reporting > Client Malware Risk**.

**Step 2** In the **Web Proxy - Client Malware Risk** section, click a user name in the "User ID / Client IP Address" column.

### What to do next

User Details Page, on page 367

# 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). |

| Section | Description |
|---|---|
| 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 of the following tabs:

| Web Tracking Page | Link to Task |
|---|---|
| Transactions processed by the Web Proxy | Searching for Transactions Processed by the Web Proxy , on page 374 |
| Transactions processed by the L4 Traffic Monitor | Searching for Transactions Processed by the L4 Traffic Monitor , on page 377 |
| Transactions processed by the SOCKS Proxy | Searching for Transactions Processed by the SOCKS Proxy , on page 377 |



**Note** A transparent request displays the name of the domain or server on the tracking page. However, when transparent requests, including transparent passthrough, are sent without SNI, the IP address is displayed.

# 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.

## Procedure

**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.<br>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.<br>**Note**<br>You can search for SNI (Server Name Indication). SNI, an extension of the TLS protocol, enables clients to securely specify hostnames while performing web transactions. You must specify entire words.<br>For SNI to work, AMP, and Reputation Services must be enabled. |
| 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.<br>To filter by an application type, select **Filter by Application Type** and choose an application type by which to filter. |

| Setting | Description |
|---|---|
| Policy | To filter by the name of the policy responsible for the final decision on this transaction, select **Filter by Action Policy** and enter a policy group name (Access Policy, Decryption Policy, or Data Security Policy) by which to filter. See the description for PolicyGroupName in the section Web Proxy Information in Access Log Files, on page 440 for more information. |
| Advanced Malware Protection | See About Web Tracking and Advanced Malware Protection Features , on page 297. |
| Malware Threat | To filter by a particular malware threat, select **Filter by Malware Threat** and enter a malware threat name by which to filter.<br>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.<br>• 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**.<br>• 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**.<br>**Note**<br>When you enable this filter, the search results include some “best guess” transactions. |
| Encapsulated URL Protection | Enable this filter for encapsulated URL transactions.<br>**Note**<br>• You must enable the HTTPS Proxy. See Enabling the HTTPS Proxy, on page 245<br>• Ensure that the web reputation score range for https://translate.google.com is set to decrypt. See Configuring Web Reputation Filter Settings for Decryption Policy Groups, on page 275 |

**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.

### What to do next

- URL Category Set Updates and Reports , on page 369
- Malware Category Descriptions, on page 279
- About Web Tracking and Advanced Malware Protection Features , on page 297

# 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.

### Procedure

**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**.

### What to do next

SOCKS Proxy Page , on page 373

# 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

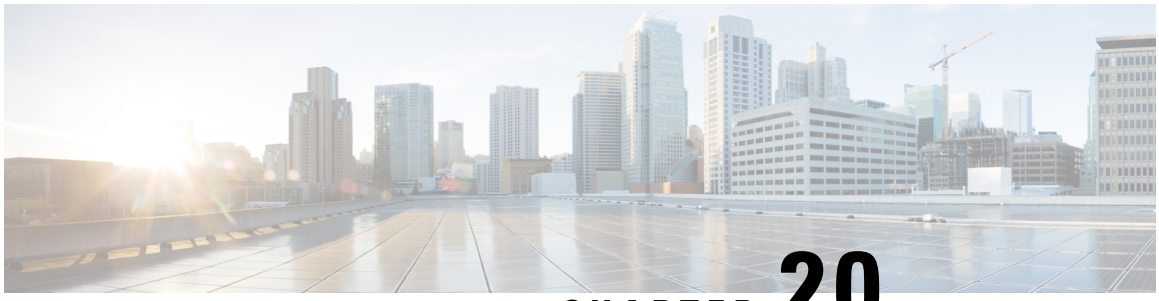
Use the **Reporting > System Status** page to monitor the System Status. This page displays the current status and configuration of the Web Security Appliance .

| This Section... | Displays |
|---|---|
| Web Security Appliance Status | • System uptime<br>• System resource utilization — CPU usage, RAM usage, and percentage of disk space used for reporting and logging.<br><br>The CPU utilization value shown on this page and the CPU value shown on the system Overview page (Overview Page, on page 365) may differ slightly because they are read separately, at differing moments.<br><br>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.<br><br>**Note**<br>Proxy Buffer Memory is one component that uses this RAM. |
| Proxy Traffic Characteristics | • Transactions per second<br>• Bandwidth<br>• Response time<br>• Cache hit rate<br>• Connections |
| Web Traffic Tap | Web Traffic Tap CPU Utilization. |

| This Section... | Displays |
|---|---|
| High Availability | Status of High Availability service. |
| External Services | • Identity Services Engine |
| Current Configuration | Web Proxy settings:<br>• Web Proxy Status — enabled or disabled.<br>• Deployment Topology.<br>• Web Proxy Mode — forward or transparent.<br>• IP Spoofing — enabled or disabled.<br>L4 Traffic Monitor settings:<br>• L4 Traffic Monitor Status — enabled or disabled.<br>• L4 Traffic Monitor Wiring.<br>• L4 Traffic Monitor Action — monitor or block.<br>Web Traffic Tap settings:<br>• Web Traffic Tap Status — enabled or disabled<br>• Web Traffic Tap Interface — P1, P2, TI, or T2<br>Web Security Appliance Version Information<br>Hardware information |

### Related Topics

System Capacity Page, on page 378



CHAPTER 20

# Secure Appliance Reports on the New Web Interface

This topic contains the following sections:


- Understanding the Web Reporting Pages on the New Web Interface, on page 381
- (Web Reports Only) Choosing Which Data to Chart, on page 404
- Web Tracking on the New Web Interface, on page 405
- Working with Web Tracking Search Results , on page 410
- Scheduling and Archiving Web Reports on the New Web Interface, on page 411
- System Status Page on the New Web Interface, on page 414


# Understanding the Web Reporting Pages on the New Web Interface

The following table lists the reports under the Reports drop-down. available in the latest supported release of AsyncOS for Web Security Appliance s under the **Reports** drop-down of the web interface. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360. If your Web Security Appliance s are running earlier releases of AsyncOS, not all of these reports are available.

***Table 9: Web Reports Drop-down Options***

| Reports Drop-down Option | Action |
|---|---|
| **General Reports** | |
| Overview Page | The Overview page provides a synopsis of the activity on your Web Security Appliance s. It includes graphs and summary tables for the incoming and outgoing transactions. For more information, see the Overview Page, on page 384. |
| Application Visibility Page | The Application Visibility page allows you to apply and view the controls that have been applied to a particular application types within the Security Management appliance and Web Security Appliance . For more information, see the Application Visibility Page, on page 385. |

| Reports Drop-down Option | Action |
|---|---|
| Layer 4 Traffic Monitor Page | Allows you to view information about malware ports and malware sites that the L4 Traffic Monitor detected during the specified time range. For more information, see the Layer 4 Traffic Monitor Page, on page 387. |
| SOCKS Proxy Page | Allows you to view data for SOCKS proxy transactions, including destinations and users. For more information, see the SOCKS Proxy Page, on page 389. |
| URL Categories Page | The URL Categories page allows you to view the top URL Categories that are being visited, including:<br>• The top URLs that have triggered a block or warning action to occur per transaction.<br>• All the URL categories during a specified time range for both completed, warned and blocked transactions. This is an interactive table with interactive column headings that you can use to sort data as you need.<br>For more information, see the URL Categories Page, on page 390. |
| Users Page | The Users page provides several web tracking links that allow you to view web tracking information for individual users.<br>From the Users page you can view how long a user, or users, on your system have spent on the internet, on a particular site or URL, and how much bandwidth that user is using.<br>From the Users page you can click on an individual user in the interactive Users table to view more details for that specific user on the User Details page.<br>The User Details page allows you to see specific information about a user that you have identified in the Users table on the Users page. From this page you can investigate individual user's activity on your system. This page is particularly useful if you are running user-level investigations and need to find out, for example, what sites your users are visiting, what Malware threats they are encountering, what URL categories they are accessing, and how much time a specific user is spending at these sites.<br>For more information, see the Users Page, on page 393.<br>For information on a specific user in your system, see the User Details Page (Web Reporting) , on page 394. |
| Web Sites Page | The Web Sites page allows you to view an overall aggregation of the activity that is happening on your managed appliances. From this page you can monitor high-risk web sites accessed during a specific time range. For more information, see the Web Sites Page, on page 396. |

| Reports Drop-down Option | Action |
|---|---|
| HTTPS Reports | The HTTPS Reports report page is an overall aggregation of the HTTP/HTTPS traffic summary (transactions or bandwidth usage) on the managed appliances. For more information, see the HTTPS Reports Page, on page 392 |
| **Threat Reports** | |
| Anti-Malware Page | The Anti-Malware page allows you to view information about malware ports and malware sites that the anti-malware scanning engine(s) detected during the specified time range. The upper part of the report displays the number of connections for each of the top malware ports and web sites. The lower part of the report displays malware ports and sites detected. For more information, see the Anti-Malware Page, on page 399. |
| Advanced Malware Protection Page | Advanced Malware Protection protects against zero-day and targeted file-based threats by obtaining the reputation of known files, analyzing behavior of certain files that are not yet known to the reputation service, and continuously evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network. For more information, see Advanced Malware Protection Page, on page 397. |
| Client Malware Risk Page | The Client Malware Risk page is a security-related reporting page that can be used to identify individual client computers that may be connecting unusually frequently to malware sites.<br>For more information, see the Client Malware Risks Page, on page 402. |
| Web Reputation Filters Page | Allows you to view reporting on Web Reputation filtering for transactions during a specified time range. For more information, see the Web Reputation Filters Page, on page 402. |

# About Time Spent

The Time Spent column in various tables represents the amount of time a user 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.

Once a transaction event is tagged as ‘viewed’, that is, a user goes to a particular URL, a ‘Time Spent’ value will start to be calculated and added as a field in the web reporting table.

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 example, if a user goes to four different domains in an active minute, the user is considered to have spent 15 seconds at each domain.

For the purposes of the time spent value, considering the following notes:

- An active user is defined as a user name or IP address that sends HTTP traffic through the appliance and has gone to a website that AsyncOS considers to be a “page view.”
- AsyncOS defines a page view as an HTTP request initiated by the user, as opposed to a request initiated by the client application. AsyncOS uses a heuristic algorithm to make a best effort guess to identify user page views.

Units are displayed in Hours:Minutes format.

# Overview Page

The **Overview** report page provides a synopsis of the activity on your Web Security Appliance s. It includes graphs and summary tables for the incoming and outgoing transactions.

To view the Overview report page, choose **Monitoring > Overview** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360.

At a high level the **Overview** report page shows you statistics about the URL and User usage, Web Proxy activity, and various transaction summaries. The transaction summaries gives you further trending details on, for example suspect transactions, and right across from this graph, how many of those suspect transactions are blocked and in what manner they are being blocked.

The lower half of the Overview report page is about usage. That is, the top URL categories being viewed, the top application types and categories that are being blocked, and the top users that are generating these blocks or warnings.

***Table 10: Details on the Overview Page***

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 356. |
| Total Web Proxy Activity | You can view the web proxy activity that is being reported by the Web Security Appliance s that are currently managed by the Security Management appliance.<br>This section displays the actual number of transactions and the approximate date that the activity occurred in graphical format.<br>You can also view the percentage of web proxy activity that are suspect, or clean proxy activity, including the total number of transactions. |
| Suspect Transactions | You can view the web transactions that have been labeled as suspect by the administrator in a graphical format.<br>This section displays the actual number of transactions and the approximate date that the activity occurred, in graphical format.<br>You can also view the percentage of blocked or warned transactions that are suspect. Additionally you can see the type of transactions that have been detected and blocked, and the actual number of times that this transaction was blocked. |

| Section | Description |
|---|---|
| L4 Traffic Monitor Summary | You can view any L4 traffic that is being reported by the Web Security Appliance s that are currently managed by the Security Management appliance, in graphical format. |
| Top URL Categories: Total Transactions | You can view the top URL categories that are being blocked, including the type of URL category and the actual number of times the specific type of category has been blocked in graphical format.<br>The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports , on page 391. |
| Top Application Types: Total Transactions | You can view the top application types that are being blocked, including the name of the actual application type and the number of times the specific application has been blocked, in graphical format. |
| Top Malware Categories: Monitored or Blocked | You can view all the Malware categories that have been detected, in graphical format. |
| Top Users: Blocked or Warned Transactions | You can view the actual users that are generating the blocked or warned transactions, in graphical format. Users can be displayed by IP address or by user name. |
| Top Threat Categories: Blocked by WBRS | You can view all the threat categories that have been blocked, in graphical format |

# Application Visibility Page



**Note** For detailed information on Application Visibility, see the 'Understanding Application Visibility and Control' topic in User Guide for AsyncOS for Cisco Web Security Appliance .

The **Application Visibility** report page allows you to apply controls to particular application types within the Security Management appliance and Web Security Appliance .

To view the Application Visibility report page, choose **Monitoring > Application Visibility** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360.

The application control gives you more granular control over web traffic than just URL filtering, for example, as well as more control over the following types of applications, and application types:

- Evasive applications, such as anonymizers and encrypted tunnels.
- Collaboration applications, such as Cisco WebEx, Facebook, and instant messaging.
- Resource intensive applications, such as streaming media.

### Understanding the Difference between Application versus Application Types

It is crucial to understand the difference between an application and an application types so that you can control the applications involved for your reports.

- **Application Types**. A category that contains one or more applications. For example, search engines is an application type that may contain search engines such as Google Search and Craigslist. Instant messaging is another application type category which may contain Yahoo Instant Messenger, or Cisco WebEx. Facebook is also an application type.
- **Applications**. Particular applications that belong in an application type. For example, YouTube is an application in the Media application type.
- **Application behaviors**. Particular actions or behaviors that users can accomplish within an application. For example, users can transfer files while using an application, such as Yahoo Messenger. Not all applications include application behaviors you can configure.

**Note** For detailed information on understanding how you can use Application Visibility and Control (AVC) engine to control Facebook activity, see the 'Understanding Application Visibility and Control' topic in User Guide for AsyncOS for Cisco Web Security Appliance s.

From the Application Visibility page, you can view the following information:

***Table 11: Details on the Application Visibility Page***

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 356. |
| Top Application Types by Total Transactions | You can view the top application types that are being visited on the site in graphical format.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404.<br><br>For example, instant messaging tools such as Yahoo Instant Messenger, Facebook, and Presentation application types. |
| Top Applications by Blocked Transactions | You can view the top application types that triggered a block action to occur per transaction in graphical format.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404.<br><br>For example, a user has tried to start a certain application type, for example Google Talk or Yahoo Instant Messenger, and because of a specific policy that is in place, this triggered a block action. This application then gets listed in this graph as a transaction blocked or warning. |

| Section | Description |
|---|---|
| Application Types Matched | The Application Types Matched interactive table allows you to view granular details about the application types listed in the Top Applications Type by Total Transactions table.<br>From the Applications column you can click on an application to view details. |
| Applications Matched | The Applications Matched interactive table shows all the application during a specified time range.<br>Additionally, you can find a specific Application within the Application Matched section. In the text field at the bottom of this section, enter the specific Application name and click Find Application. |

# Layer 4 Traffic Monitor Page

The **Layer 4 Traffic Monitor** report page displays information about malware ports and malware sites that the Layer 4 Traffic Monitors on your Web Security Appliance s have detected during the specified time range. It also displays IP addresses of clients that frequently encounter malware sites.

To view the Web Sites report page, choose **Monitoring > Web Sites** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360.

The Layer 4 Traffic Monitor listens to network traffic that comes in over all ports on each Web Security Appliance and matches domain names and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic.

You can use data in this report to determine whether to block a port or a site, or to investigate why a particular client IP address is connecting unusually frequently to a malware site (for example, this could be because the computer associated with that IP address is infected with malware that is trying to connect to a central command and control server.)

***Table 12: Details on the Layer 4 Traffic Monitor Page***

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 356. |
| Top Client IPs: Malware Connections Detected | You can view the top IP addresses of computers in your organization that most frequently connect to malware sites, in graphical format.<br>To customize the view of the chart, click  on the chart. For more information, see Choosing Which Data to Chart , on page 357.<br>This chart is the same as the “Layer 4 Traffic Monitor: Malware Connections Detected” chart on the Client Malware Risks Page, on page 402. |

| Section | Description |
|---|---|
| Top Malware Sites: Malware Connections Detected | You can view the top malware domains detected by the Layer 4 Traffic Monitor, in graphical format.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see Choosing Which Data to Chart , on page 357. |
| Client Source IPs | You can use the this interactive table to view the IP addresses of computers in your organization that frequently connect to malware sites.<br><br>To include only data for a particular port, enter a port number into the box at the bottom of the table and click Filter by Client IP. You can use this feature to help determine which ports are used by malware that "calls home" to malware sites.<br><br>To view details such as the port and destination domain of each connection, click an entry in the table. For example, if one particular client IP address has a high number of Malware Connections Blocked, click the number in that column to view a list of each blocked connection. The list is displayed as search results in the Layer 4 Traffic Monitor tab of the Web Tracking Search page. For more information about this list, see Searching for Transactions Processed by the Layer 4 Traffic Monitor, on page 409.<br><br>This chart is the same as the "Layer 4 Traffic Monitor: Malware Connections Detected" chart on the Client Malware Risks Page, on page 402. |
| Malware Ports | You can use the this interactive table to view the ports on which the Layer 4 Traffic Monitor has most frequently detected malware.<br><br>To view details, click an entry in the table. For example, click the number of Total Malware Connections Detected to view details of each connection on that port. The list is displayed as search results in the Layer 4 Traffic Monitor tab on the Web Tracking Search page. For more information about this list, see Searching for Transactions Processed by the Layer 4 Traffic Monitor, on page 409. |
| Malware Sites Detected | You can use the this interactive table to view the domains on which the Layer 4 Traffic Monitor most frequently detects malware.<br><br>To include only data for a particular port, enter a port number into the box at the bottom of the table and click Filter by Port. You can use this feature to help determine whether to block a site or a port.<br><br>To view details, click an entry in the table. For example, click the number of Malware Connections Blocked to view the list of each blocked connection for a particular site. The list is displayed as search results in the Layer 4 Traffic Monitor tab on the Web Tracking Search page. For more information about this list, see Searching for Transactions Processed by the Layer 4 Traffic Monitor, on page 409. |

### Related Topics

Troubleshooting L4 Traffic Monitor Reports , on page 364

# SOCKS Proxy Page

The SOCKS Proxy report page allows you to view transactions processed through the SOCKS proxy, including information about destinations and users, in a graphical and tabular format.

To view the SOCKS Proxy report page, choose **Monitoring > SOCKS Proxy** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360.

**Note** The destination shown in the report is the address that the SOCKS client (typically a browser) sends to the SOCKS proxy.

To change SOCKS policy settings, see *User Guide for AsyncOS for Cisco Web Security Appliance s*.

***Table 13: Details on the SOCKS Proxy Page***

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 356. |
| Top Destinations for SOCKS: Total Transactions | You can view the top destinations detected by the SOCKS proxy, in graphical format.<br><br>To customize the view of the chart, click on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404. |
| Top Users for SOCKS: Malware Transactions | You can view the top users detected by the SOCKS proxy, in graphical format.<br><br>To customize the view of the chart, click on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404. |
| Destinations | You can use the this interactive table to view the list of destination domains or IP addresses processed through SOCKS proxy.<br><br>To include only data for a particular destination, enter a domain name or IP address into the box at the bottom of the table and click **Find Domain or IP**. |
| Users | You can use the this interactive table to view the list of users or IP addresses processed through SOCKS proxy.<br><br>To include only data for a particular user, enter a user name or IP address into the box at the bottom of the table and click **Find User ID / Client IP Address**. |

### Related Topics

Searching for Transactions Processed by the SOCKS Proxy , on page 409

# URL Categories Page

The **URL Categories** report page can be used to view the URL categories of sites that users on your system are visiting.

To view the URL Categories report page, choose **Monitoring > URL Categories** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360.

From the URL Categories page, you can view the following information:

***Table 14: Details on the URL Categories Page***

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 356. |
| Top URL Categories: Total Transactions | You can view the top URL Categories that are being visited on the site in a graphical format.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404. |
| Top URL Categories: Blocked and Warned Transactions | You can view the top URL that triggered a block or warning action to occur per transaction in a graphical format. For example, a user went to a certain URL and because of a specific policy that is in place, this triggered a block action or a warning. This URL then gets listed in this graph as a transaction blocked or warning.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404. |
| Top Youtube Categories : Total Transactions | You can view the top Youtube Categories that are being visited on the site in a graphical format.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404. |

| Section | Description |
|---|---|
| Top Youtube Categories : Blocked and Warned Transactions | You can view the top Youtube URL that triggered a block or warning action to occur per transaction in a graphical format. For example, a user went to a certain Youtube URL and because of a specific policy that is in place, this triggered a block action or a warning. This Youtube URL then gets listed in this graph as a transaction blocked or warning.<br><br>To customize the view of the chart, click  on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404. |
| URL Categories Matched | The URL Categories Matched interactive table shows the disposition of transactions by URL category during the specified time range, plus bandwidth used and time spent in each category.<br><br>If there are a large number of unclassified URLs, see Reducing Uncategorized URLs , on page 391. |

## Reducing Uncategorized URLs

If the percentage of uncategorized URLs is higher than 15-20%, consider the following options:

- For specific localized URLs, you can create custom URL categories and apply them to specific users or group policies. These transactions will then be included in “URL Filtering Bypassed” statistics instead. To do this, see information about custom URL categories AsyncOS for Cisco Web Security Appliance s User Guide.
- For sites that you feel should be included in existing or other categories, see Reporting Misclassified and Uncategorized URLs , on page 392.

## 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.

## Using The URL Categories Page in Conjunction with Other Reporting Pages

The URL Categories page can be used in conjunction with the Application Visibility Page, on page 385, the User Details Page (Web Reporting) , on page 394and the Users Page, on page 393 to investigate a particular user and the types of applications or websites that a particular user is trying to access.

For example, from the URL Categories Page, on page 390, you can generate a high level report for Human Resources which details all the URL categories that are visited by the site. From the same page, you can gather further details in the URL Categories interactive table about the URL category ‘Streaming Media’. By clicking on the Streaming Media category link, you can view the specific URL Categories report page. This page not only displays the top users that are visiting streaming media sites (in the Top Users by Category for Total

Transactions section), but also displays the domains that are visited (in the Domains Matched interactive table) such as YouTube.com or QuickPlay.com.

At this point, you are getting more and more granular information for a particular user. Now, let's say this particular user stands out because of their usage, and you want to find out exactly what they are accessing. From here you can click on the user in the Users interactive table. This action takes you to the Users Page, on page 393, where you can view the user trends for that user, and find out exactly what they have been doing on the web.

If you wanted to go further, you can now get down to web tracking details by clicking on Transactions Completed link in the interactive table. This displays the Searching for Transactions Processed by Web Proxy Services, on page 405 on the Web Tracking page where you can see the actual details about what dates the user accessed the sites, the full URL, the time spent on that URL, etc.

## Reporting Misclassified and Uncategorized URLs

You can report misclassified and uncategorized URLs at the following URL:

https://talosintelligence.com/tickets.

Submissions are evaluated for inclusion in subsequent rule updates.

To check the status of submitted URLs, click the **Status on Submitted URLs** tab on this page.

# HTTPS Reports Page

The HTTPS Reports report page is an overall aggregation of the HTTP/HTTPS traffic summary (transactions or bandwidth usage) on the managed appliances.

You can also view the summary of supported ciphers based on either client side connections or server side connections, for individual HTTP/HTTPS web traffic that passes through the managed appliance.

To view the HTTPS Reports report page, choose **Monitoring > HTTPS Reports** from the **Reports** drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360.

***Table 15: Details on the HTTPS Reports Page***

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Changing the Time Range, on page 355. |
| Web Traffic Summary | You can view the web traffic summary on the appliance in one of the following ways:<br>• **Transactions**: Select this option from the drop-down list to display the web traffic summary based on the number of HTTP or HTTPS web transactions, in a graphical format and percentage of HTTP or HTTPS web transaction in tabular format.<br>• **Bandwidth Usage**: Select this option from the drop-down list to display the web traffic summary based on the amount of bandwidth consumed by the HTTP or HTTPS web traffic, in a graphical format and the percentage of HTTP or HTTPS bandwidth usage in tabular format. |

| Section | Description |
|---|---|
| Trend: Web Traffic | You can view the trend graph for the web traffic on the appliance based on the required time range in one of the following ways:<br>• **Web Traffic Trend**: Select this option from the dropdown list to display the cumulative trend for HTTP and HTTPS web traffic based on the transactions or bandwidth usage.<br>• **HTTPS Trend**: Select this option from the dropdown list to display the trend for HTTPS web traffic based on the transactions or bandwidth usage.<br>• **HTTP Trend**: Select this option from the dropdown list to display the trend for HTTP web traffic based on the transactions or bandwidth usage. |
| Ciphers | You can view the summary of the ciphers in one of the following ways:<br>• **By Client Side Connections**: Select this option from the dropdown list to display the summary of the ciphers used on the client side of the HTTP or HTTPS web traffic in a graphical format.<br>• **By Server Side Connections**: Select this option from the dropdown list to display the summary of the ciphers used on the server side of the HTTP or HTTPS web traffic in a graphical format. |

# Users Page

The **Users** report page provides several links that allow you to view web reporting information for individual users.

To view the Users report page, choose **Monitoring > Users** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360.

From the **Users** page you can view how long a user, or users, on your system have spent on the internet, on a particular site or URL, and how much bandwidth that user is using.

**Note** The maximum number of users on the Web Security Appliance that the Security Management appliance can support is 500.

From the **Users** page, you can view the following information pertaining to the users on your system:

***Table 16: Details on the Users Page***

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 356. |

| Section | Description |
|---|---|
| Top Users: Transactions Blocked | You can view the top users, by either IP address or user name, and the number of transactions that have been blocked specific to that user, in graphical format. The user name or IP address can be made unrecognizable for reporting purposes. For more information on how to make user names unrecognizable in for this page or in scheduled reports, see the *User Guide for AsyncOS for Cisco Content Security Management Appliances*. The default setting is that all user names appear.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404. |
| Top Users: Bandwidth Used | You can view the top users, by either IP address or user name, that are using the most bandwidth on the system, in graphical format.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404. |
| Users | You can use this interactive table to search for a specific User ID or Client IP address. In the text field at the bottom of the User table, enter the specific User ID or Client IP address and click on Find User ID / Client IP Address. The IP address does not need to be an exact match to return results.<br><br>You can click on a specific user to find more specific information. For more information, see the User Details Page (Web Reporting) , on page 394 |

**Note** To view user IDs instead of client IP addresses, you must set up your Security Management appliance to obtain user information from an LDAP server.

## User Details Page (Web Reporting)

The **User Details** page allows you to see specific information about a user that you have identified in the interactive table on the Users report page.

The User Details page allows you to investigate individual user's activity on your system. This page is particularly useful if you are running user-level investigations and need to find out, for example, what sites your users are visiting, what Malware threats they are encountering, what URL categories they are accessing, and how much time a specific user is spending at these sites.

To display the User Details page for a specific user, click on a specific user from the Users interactive table on the **Users** report page.

From the User Details page, you can view the following information pertaining to an individual user on your system:

*Table 17: Details on the User Details Page*

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 356. |
| URL Categories: Total Transactions | You can view the specific URL Categories that a specific user is using, in graphical format.<br><br>To customize the view of the chart, click ✓ on the chart.<br><br>The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports , on page 369. |
| Trend: Total Transactions | You can use this trend graph to view all the web transactions of a specific user.<br><br>To customize the view of the chart, click ✓ on the chart.<br><br>For example, this graph will indicate if there is a large spike in web traffic during certain hours of the day, and when those spikes occur. Using the Time Range drop-down list, you can expand this graph to see a more or less granular span of time that this user was on the web. |
| URL Categories Matched | The URL Categories Matched interactive table shows matched categories for both completed and blocked transactions.<br><br>You can search for a specific URL Category in the text field at the bottom of the table and click **Find URL Category**. The category does not need to be an exact match.<br><br>The set of predefined URL categories is occasionally updated. For more information about the impact of these updates on report results, see URL Category Set Updates and Reports , on page 369. |
| Domains Matched | The Domains Matched interactive table shows domains or IP addresses that the user has accessed. You can also view the time spent on those categories, and various other information that you have set from the column view.<br><br>You can search for a specific Domain or IP address in the text field at the bottom of the table and click **Find Domain or IP**. The domain or IP address does not need to be an exact match. |
| Applications Matched | The Applications Matched interactive table shows applications that a specific user is using. For example, if a user is accessing a site that requires use of a lot of Flash video, you will see the application type in the Application column.<br><br>You can search for a specific application name in the text field at the bottom of the table and click **Find Application**. The name of the application does not need to be an exact match. |

| Section | Description |
|---|---|
| Advanced Malware Protection Threats Detected | The Advanced Malware Protection Threats Detected interactive table shows malware threat files that are detected by the Advanced Malware Protection engine.<br>You can search for data on a specific SHA value of the malware threat file, in the text field at the bottom of the table and click **Find malware Threat File SHA 256**. The name of the application does not need to be an exact match. |
| Malware Threats Detected | The Malware Threats Detected interactive table shows the top Malware threats that a specific user is triggering.<br>You can search for data on a specific malware threat name in the text field at the bottom of the table and click **Find Malware Threat**. The name of the Malware Threat does not need to be an exact match. |
| Policies Matched | The Policies Matched interactive table shows the policy groups that applied to this user when accessing the web.<br>You can search for a specific policy name in the text field at the bottom of the table and click **Find Policy**. The name of the policy does not need to be an exact match. |

**Note** From Client Malware Risk Details table: The client reports sometimes show a user with an asterisk (*) at the end of the user name. For example, the Client report might show an entry for both “jsmith” and “jsmith*”. User names listed with an asterisk (*) indicate the user name provided by the user, but not confirmed by the authentication server. This happens when the authentication server was not available at the time and the appliance is configured to permit traffic when authentication service is unavailable.

# Web Sites Page

The **Web Sites** report page is an overall aggregation of the activity that is happening on the managed appliances. You can use this report page to monitor high-risk web sites accessed during a specific time range.

To view the Web Sites report page, choose **Monitoring > Web Sites** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360.

From the Web Sites page, you can view the following information:

***Table 18: Details on the Web Sites Page***

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 356. |

| Section | Description |
|---|---|
| Top Domains: Total Transactions | You can view the top domains that are being visited on the website in graphical format.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404. |
| Top Domains: Transactions Blocked | You can view the top domains that triggered a block action to occur per transaction in graphical format.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404.<br><br>For example, a user went to a certain domain and because of a specific policy that I have in place, this triggered a block action. This domain is listed in this graph as a transaction blocked, and the domain site that triggered the block action is listed. |
| Domains Matched | You can use this interactive table to search for the domains that are that are being visited on the website. You can click on a specific domain to access more granular information. The Proxy Services tab on the Web Tracking page appears and you can see tracking information and why certain domains were blocked.<br><br>When you click on a specific domain you can see the top users of that domain, the top transactions on that domain, the URL Categories matched and the Malware threats that have been detected. |

# Advanced Malware Protection Page

Advanced Malware Protection protects against zero-day and targeted file-based threats by:

- Obtaining the reputation of known files.
- Analyzing behavior of certain files that are not yet known to the reputation service.
- Evaluating emerging threats as new information becomes available, and notifying you about files that are determined to be threats after they have entered your network.

For more information on the file reputation filtering and file analysis, see the user guide or online help for *AsyncOS for Web Security Appliance s*.

The  Advanced Malware Protection report page shows the following reporting views:

- Advanced Malware Protection–Summary Page
- Advanced Malware Protection–File Analysis Page

To view the Advanced Malware Protection report page, choose **Monitoring > Advanced Malware Protection** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360.

## Advanced Malware Protection - AMP Summary Page

The AMP Summary section of the Advanced Malware Protection report page shows file-based threats that were identified by the file reputation service.

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.

You can click on the link in the Malware Threat Files interactive table to view all the 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.

If a file extracted from a compressed or archived file is malicious, only the SHA value of the compressed or archived file is included in the Advanced Malware Protection report.

You can use the AMP Summary section of the Advanced Malware Protection page to view:

- The summary of files that are identified by file reputation service of the Advanced Malware Protection engine, in a graphical format.
- The top malware threat files in a graphical format.
- The top threat files based on the file types in a graphical format.
- A trend graph for all the malware threat files based on the selected time range.
- The Malware Threat Files interactive table that lists the top malware threat files.
- The Files With Retrospective Verdict Change interactive table that lists the files processed by this appliance for which the verdict has changed since the transaction was processed. For more information about this situation, see the documentation for your Web Security Appliance .

  In the case of multiple verdict changes for a single SHA-256, this report shows only the latest verdict, not the verdict history.

  If multiple Web Security Appliance s have different verdict updates for the same file, the result with the latest time stamp is displayed.

  You can click on a SHA-256 link to view web tracking results for all transactions that included this SHA-256 within the maximum available time range, regardless of the time range selected for the report.

## Advanced Malware Protection - File Analysis Page

The File Analysis section of the Advanced Malware Protection report page shows the time and verdict (or interim verdict) for each file sent for analysis. The appliance checks for analysis results every 30 minutes.

For deployments with an on-premises Cisco AMP Malware Analytics Appliance: Files that are on the allowed list on the Cisco AMP Malware Analytics appliance show as "clean." For information about allowed listing, see the AMP Malware Analytics online help.

Drill down to view detailed analysis results, including the threat characteristics and score for each file.

You can also view additional details about an SHA directly on the server that performed the analysis by searching for the SHA or by clicking the Cisco AMP Malware Analytics link at the bottom of the file analysis details page.

If a file extracted from a compressed or archived file is sent for analysis, only the SHA value of the extracted file is included in the File Analysis report.

You can use the File Analysis section of the  Advanced Malware Protection report page to view:

- The number of files that are uploaded for file analysis by file analysis service of the  Advanced Malware Protection engine.
- A list of files that have completed file analysis requests.
- A list of files that have pending file analysis requests.

# Anti-Malware Page

The **Anti-Malware** report page is a security-related reporting page that reflects the results of scanning by your enabled scanning engines (Webroot, Sophos, McAfee, and/or Adaptive Scanning).

To view the Anti-Malware report page, choose **Monitoring** > **Anti-Malware** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360.

You can use this page to help identify and monitor web-based malware threats.

**Note** To view data for malware found by L4 Traffic Monitoring, see Layer 4 Traffic Monitor Page, on page 387

From the Anti-Malware page, you can view the following information:

***Table 19: Details on the Anti-Malware Page***

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 356. |
| Top Malware Categories | You can view the top malware categories that are detected by a given category type, in graphical format. See Malware Category Descriptions, on page 400 for more information on valid Malware categories.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404. |
| Top Malware Threats | You can view the the top malware threats in graphical format.<br><br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404. |

| Section | Description |
|---|---|
| Malware Categories | The Malware Categories interactive table shows detailed information about particular malware categories that are displayed in the Top Malware Categories chart.<br>Clicking on any of the links in the Malware Categories interactive table allows you to view more granular details about individual malware categories and where they are on the network.<br>Exception: an Outbreak Heuristics link in the table lets you view a chart showing when transactions in this category occurred.<br>See Malware Category Descriptions, on page 400 for more information on valid Malware categories. |
| Malware Threats | The Malware Threats interactive table shows detailed information about particular malware threats that are displayed in the Top Malware Threats section.<br>Threats labeled "Outbreak" with a number are threats identified by the Adaptive Scanning feature independently of other scanning engines. |

## Malware Category Report Page

### Procedure

**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

The Malware Threat Report page shows clients at risk for a particular threat, displays a list of potentially infected clients, and links to the Client Detail page. The trend graph at the top of the report shows monitored and blocked transactions for a threat during the specified time range. The table at the bottom shows the actual number of monitored and blocked transactions for a threat during the specified time range.

To view this report, click a category in the Malware Category column of the Anti-Malware report page.

For additional information, click the **Support Portal Malware Details** link below the table.

## Malware Category Descriptions

The Web Security Appliance  can block the following types of malware:

| Malware Type | Description |
|---|---|
| Adware | Adware encompasses all software executables and plug-ins that direct users towards products for sale. Some adware applications have separate processes that run concurrently and monitor each other, ensuring that the modifications are permanent. Some variants enable themselves to run each time the machine is started. These programs may also change security settings making it impossible for users to make changes to their browser search options, desktop, and other system settings. |
| Browser Helper Object | A browser helper object is 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, meaningful, and informed 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 user's full, meaningful, and informed consent. |
| 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. |
| Outbreak Heuristics | This category represents malware found by Adaptive Scanning independently of the other anti-malware engines. |
| 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. Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal personal identity data and financial account credentials. |
| PUA | Potentially Unwanted Application. A PUA is an application that is not malicious, but which may be considered to be undesirable. |
| System Monitor | A system monitor encompasses any software that performs one of the following actions:<br>Overtly or covertly records system processes and/or user action.<br>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. These installations usually occur without the user's knowledge. Additionally, a Trojan Downloader's payload may differ from installation to installation since it obtains downloading instructions from the remote host/site. |
| Trojan Horse | A trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves. |

| Malware Type | Description |
|---|---|
| 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 for bank sites, auction sites, or online payment sites. |
| Virus | A virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. |
| Worm | A worm is program or algorithm that replicates itself over a computer network and usually performs malicious actions. |

# Client Malware Risks 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).

***Table 20: Details on Client Malware Risks Page***

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 356. |
| Web Proxy: Top Clients Monitored or Blocked | 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: Client Malware Risk | The Web Proxy: Client Malware Risk interactive 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 | The L4 Traffic Monitor: Clients by Malware Risk interactive table displays IP addresses of computers in your organization that frequently connect to malware sites. |

# Web Reputation Filters Page

You can use the **Web Reputation Filters** report page to view the results of your set Web Reputation filters for transactions during a specified time range.

To view the Web Reputation Filters report page, choose **Monitoring** > **Web Reputation Filters** from the Reports drop-down. For more information, see Using the Interactive Report Pages on the New Web Interface, on page 360.

### What are Web Reputation Filters?

Web Reputation Filters analyze web server behavior and assign a reputation score to a URL to determine the likelihood that it contains URL-based malware. It helps protect against URL-based malware that threatens end-user privacy and sensitive corporate information. The Web Security Appliance uses URL reputation scores to identify suspicious activity and stop malware attacks before they occur. You can use Web Reputation Filters with both Access and Decryption Policies.

Web Reputation Filters use statistical data to assess the reliability of Internet domains and score the reputation of URLs. Data such as how long a specific domain has been registered, or where a web site is hosted, or whether a web server is using a dynamic IP address is used to judge the trustworthiness of a given URL.

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

For more information on Web Reputation Filtering, see 'Web Reputation Filters' in the *User Guide for AsyncOS for Web Security Appliance s*.

From the Web Reputation Filters page, you can view the following information:

***Table 21: Details on Web Reputation Filters Page***

| Section | Description |
|---|---|
| Time Range (drop-down list) | Choose the time range for your report. For more information, see the Choosing a Time Range for Reports, on page 356. |
| Web Reputation Actions (Trend) | You can view the total number of web reputation actions against the time specified, in graphical format. From this you can see potential trends over time for web reputation actions. |

| Section | Description |
|---|---|
| Web Reputation Actions (Volume) | You can view the web reputation action volume in percentages by transactions. |
| Web Reputation Threat Types Blocked by WBRS | You can view the types of threats found in transactions that were blocked by Web Reputation filtering, in graphical format.<br>**Note**<br>WBRS cannot always identify the threat type. |
| Threat Types Detected in Other Transactions | You can view the type of threats found in transactions that were not blocked by Web Reputation filtering, in graphical format.<br>To customize the view of the chart, click ✓ on the chart. For more information, see (Web Reports Only) Choosing Which Data to Chart, on page 404.<br>Reasons these threats might not have been blocked include:<br>• Not all threats have a score that meets the threshold for blocking. However, other features of the appliance may catch these threats.<br>• Policies might be configured to allow threats to pass through.<br>**Note**<br>WBRS cannot always identify the threat type. |
| Web Reputation Actions (Breakdown by Score) | If Adaptive Scanning is not enabled, this interactive table displays the Web Reputation scores broken down for each action. |
| Threat Categories Matched | You can view the threat categories matched, in graphical format. |

### Adjusting Web Reputation Settings

Based on your report results, you may want to adjust the configured web reputation settings, for example adjust the threshold scores or enable or disable Adaptive Scanning. For specific information about configuring web reputation settings, see *User Guide for AsyncOS for Cisco Web Security Appliance s*.

# (Web Reports Only) 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.

Generally, the chart options are the same as the columns of the table in the report. However, some columns cannot be charted.

Charts reflect all available data in a table column, regardless of the number of items (rows) you choose to display in the associated table.

**Procedure**

**Step 1** Click  on a specific chart.

**Step 2** Choose the required data to be displayed. The preview of the chart is displayed as per the selected options.

**Step 3** Click **Apply**.

# Web Tracking on the New Web Interface

You can use the **Web Tracking Search** page to search and view details about individual transactions or patterns of transactions that may be of concern. Depending on the services that your deployment uses, search in relevant tabs:

- Searching for Transactions Processed by Web Proxy Services, on page 405
- Searching for Transactions Processed by the Layer 4 Traffic Monitor, on page 409
- Searching for Transactions Processed by the SOCKS Proxy , on page 409
- Working with Web Tracking Search Results , on page 410
- Viewing Transaction Details for Web Tracking Search Results , on page 411

For more information about the distinction between the Web Proxy and the Layer4 Traffic Monitor, see the "Understanding How the Web Security Appliance  Works" section in *User Guide for AsyncOS for Cisco Web Security Appliance s.*

## Searching for Transactions Processed by Web Proxy Services

You can use the **Proxy Services** tab on the **Web Tracking Search** page to search web tracking data aggregated from individual security components and acceptable use enforcement components. This data does not include Layer 4 Traffic Monitoring data or transactions processed by the SOCKS Proxy.

You might want to use it to assist the following roles:

- **HR or Legal manager.** Run an investigative report for an employee during a specific time period.

  For example, you can use the Proxy Services tab to retrieve information about a specific URL that a user is accessing, what time the user visited that URL, whether that URL is allowed, etc.

- **Network security administrator.** Examine whether the company network is being exposed to malware threats through employees' smartphones.

You can view search results for the transactions recorded (including 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.

For an example of how the Proxy Services tab can be used with other web reporting pages, see the .

## Procedure

**Step 1** On the Security Management appliance, choose **Web** from the dropdown list..

**Step 2** Using The URL Categories Page in Conjunction with Other Reporting Pages, on page 391 Choose **Tracking > Proxy Services**.

**Step 3** To see all search and filtering options, click **Advanced**.

**Step 4** Enter search criteria:

*Table 22: Web Tracking Search Criteria on the Proxy Services Tab*

| Option | Description |
|---|---|
| Default Search Criteria | |
| Time Range | Choose the time range on which to report. For information on time ranges available on the Security Management appliance, see the Choosing a Time Range for Reports, on page 356. |
| User/Client IPv4 or IPv6 | Optionally, 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, such as 172.16.0.0/16.<br>When you leave this field empty, the search returns results for all users. |
| Website | Optionally, 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. |
| Advanced Search Criteria | |
| URL Category | To filter by a URL category, select **Filter by URL Category** and type the first letter of a custom or predefined URL category by which to filter. Choose the category from the list that appears .<br>All recent transactions that match the category name are included, regardless of the engine name noted in the drop-down list. |
| Malware Threat | To filter by a particular malware threat, select **Filter by Malware Threat** and enter a malware threat name by which to filter.<br>To filter by a malware category, select **Filter by Malware Category** and choose a malware category by which to filter. For descriptions, see Malware Category Descriptions, on page 400. |

| Option | Description |
|---|---|
| Application | To filter by an application, select **Application** and choose an application by which to filter.<br>To filter by an application type, select **Application Type** and choose an application type by which to filter. |
| WBRS | In the WBRS section, you can filter by Web-Based Reputation Score and by a particular web reputation threat.<br>• 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**.<br>• To filter by web reputation threat, select **Filter by Reputation Threat** and enter a web reputation threat by which to filter.<br>For more information on WBRS scores, see the IronPort AsyncOS for Web User Guide. |
| Threat Category | To filter by a specific threat category, expand the **Threat Category** section and select the threat categories that you want.<br>To select all available threat categories, click **Select All**. |
| Youtube Category | To filter by a specific Youtube category, expand the **Youtube Category** section and select the Youtube categories that you want to view.<br>To select all available Youtube categories, click **Select All**. You can also filter by Acitve and Inactive categories. |
| Policy | To filter by a policy group, select **Policy** and enter a policy group name by which to filter.<br>Make sure that you have declared the policy on the Web Security Appliance . |
| AnyConnect Secure Mobility | To filter by remote or local access, select **User Location** and choose an access type. To include all access types, select **Disable Filter**.<br>(In previous releases, this option was labeled Mobile User Security.) |
| Advanced Malware Protection | To filter file-based threats identified by the file reputation service, enter a filename in the **Filename** box.<br>To filter files using the SHA-256 hash, enter a SHA-256 has value in the **File SHA-256** box.<br>To filter files based on file verdict, select AMP **File Verdict** and choose a verdict type. The available file verdict types are **Clean**, **Malicious**, **Unknown**, **UnScannable**, and **Lowrisk**.<br>The **Malicious** verdict type has three sub-cateogries:<br>• **Malware**: Files that are blocked due to reasons other than Custom Detection nor Custom Threshold.<br>• **Custom Detection**: The percentage of file SHAs on the blocked list received from the AMP for Endpoints console.<br>• **Custom Threshold**: The files blocked due to Threshold Settings while configuring AMP. |

| Option | Description |
|---|---|
| User Request | To filter by transactions that were actually initiated by the user, select **Filter by Web User-Requested Transactions**.<br>**Note:** When you enable this filter, the search results include “best guess” transactions. |

## Malware Category Descriptions

The Web Security Appliance  can block the following types of malware:

| Malware Type | Description |
|---|---|
| Adware | Adware encompasses all software executables and plug-ins that direct users towards products for sale. Some adware applications have separate processes that run concurrently and monitor each other, ensuring that the modifications are permanent. Some variants enable themselves to run each time the machine is started. These programs may also change security settings making it impossible for users to make changes to their browser search options, desktop, and other system settings. |
| Browser Helper Object | A browser helper object is 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, meaningful, and informed 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 user’s full, meaningful, and informed consent. |
| 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. |
| Outbreak Heuristics | This category represents malware found by Adaptive Scanning independently of the other anti-malware engines. |
| 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. Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal personal identity data and financial account credentials. |
| PUA | Potentially Unwanted Application. A PUA is an application that is not malicious, but which may be considered to be undesirable. |

| Malware Type | Description |
|---|---|
| System Monitor | A system monitor encompasses any software that performs one of the following actions:<br>Overtly or covertly records system processes and/or user action.<br>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. These installations usually occur without the user's knowledge. Additionally, a Trojan Downloader's payload may differ from installation to installation since it obtains downloading instructions from the remote host/site. |
| 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 for bank sites, auction sites, or online payment sites. |
| Virus | A virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. |
| Worm | A worm is program or algorithm that replicates itself over a computer network and usually performs malicious actions. |

# Searching for Transactions Processed by the Layer 4 Traffic Monitor

The Layer 4 Traffic Monitor tab on the **Web Tracking Search** 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
- IP address of the machine that initiated the transaction (IPv4 or IPv6)
- Domain or IP address of the destination website (IPv4 or IPv6)
- Port
- IP address associated with a computer in your organization
- Connection type

To view the hostname at the questionable site or the Web Security Appliance that processed the transaction, click the Display Details link in the Destination IP Address column heading.

For more information about how you can use this information, see Layer 4 Traffic Monitor Page, on page 387.

# Searching for Transactions Processed by the SOCKS Proxy

You can search for transactions that meet a variety of criteria, including blocked or completed transactions; IP address of the client machine that initiated the transaction; and destination domain, IP address, or port. You

can also filter results by custom URL category, policy matched, and user location (local or remote). IPv4 and IPv6 addresses are supported.

**Procedure**

**Step 1** Choose **Tracking > SOCKS Proxy**.

**Step 2** To see all search and filtering options, click **Advanced**.

**Step 3** Enter search criteria.

**Step 4** Click **Search**.

**What to do next**

**Related Topics**

SOCKS Proxy Page, on page 389

# Working with Web Tracking Search Results


- Displaying More Web Tracking Search Results , on page 410
- Understanding Web Tracking Search Results , on page 410
- Viewing Transaction Details for Web Tracking Search Results , on page 411
- About Web Tracking and Upgrades , on page 411


## Displaying More Web Tracking Search Results

**Procedure**

**Step 1** Be sure to review all pages of returned results.

**Step 2** To display more results per page than the current number displayed, select an option from the **Items Displayed** menu.

**Step 3** If more transactions match your criteria than the maximum number of transactions offered in the Items Displayed menu, you can view the complete set of results by clicking the **Printable Download** link to obtain a CSV file that includes all matching transactions.

This CSV file includes the complete set of raw data, excluding details of related transactions.

## Understanding Web Tracking Search Results

By default, results are sorted by time stamp, with the most recent result at the top.

Search results include:

- The time that the URL was accessed.

- The number of related transactions spawned by the user-initiated transaction, such as images loaded, javascripts run, and secondary sites accessed. The number of related transactions appears in each row below the Display All Details link in the column heading.
- The disposition (The result of the transaction. If applicable, shows the reason the transaction was blocked, monitored, or warned.)

## Viewing Transaction Details for Web Tracking Search Results

| To View | Do This |
|---|---|
| The full URL for a truncated URL in the list | Note which host Web Security Appliance processed the transaction, then check the Accesslog on that appliance. |
| Details for an individual transaction | Click a URL in the Website column. |
| Details for all transactions | Click the **Display All Details...** link in the Website column heading. |
| A list of up to 500 related transactions | The number of related transactions appears in parentheses below the "Display Details" link in the column heading in the list of search results.<br>Click the **Related Transactions** link in the Details view for a transaction. |

## About Web Tracking and Upgrades

New web tracking features may not apply to transactions that occurred before upgrade, because the required data may not have been retained for those transactions. For possible limitations related to web tracking data and upgrades, see the Release Notes for your release.

# Scheduling and Archiving Web Reports on the New Web Interface

This section includes the following:

- Scheduling Web Reports on the New Web Interface, on page 411
- Archiving Web Reports on the New Web Interface, on page 413

## Scheduling Web Reports on the New Web Interface

This section includes the following:

- Adding Scheduled Web Reports on the New Web Interface, on page 412
- Editing Scheduled Web Reports on the New Web Interface, on page 413
- Deleting Scheduled Web Reports on the New Web Interface, on page 413

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, previous month, previous calendar day (up to 250), previous calendar month (up to 12). Alternatively, you can include data for a custom number of days (from 2 days to 100 days) or a custom number of months (from 2 months to 12 months).

Regardless of when you run a report, the data is returned from the previous time interval (hour, day, week, or month). For example, if you schedule a daily report to run at 1AM, the report will contain data from the previous day, midnight to midnight (00:00 to 23:59).

You can define as many recipients for reports as you want, including zero recipients. If you do not specify an email recipient, the system will still archive the reports. If you need to send the reports to a large number of addresses, however, you may want to create a mailing list instead of listing the recipients individually.

## Adding Scheduled Web Reports on the New Web Interface

### Procedure

**Step 1** Choose **Monitoring > Schedule & Archive**.

**Step 2** In the Schduled / Archived tab, click the + button.

**Step 3** Select your report type from the **Report Type** drop-down menu.

**Step 4** In the **Report Title** field, enter the title of your report.

To avoid creating multiple reports with the same name, we recommend using a descriptive title.

**Step 5** Choose the time range for the report from the **Time Range to Include** drop-down menu.

**Step 6** Choose the format for the generated report.

The default format is PDF.

**Step 7** From the Delivery Options section, choose any one of the following:

By choosing this, the report will be listed on the Archived Reports page.

**Note**
Domain-Based Executive Summary reports cannot be archived.

- To archive the report, select **Only Archive**.
- To archive and email the report, click **Archive and Email to Recipients**.
- To email the report, click **Only Email to Recipients**.

In the **Email IDs** field, enter the recipient email addresses.

**Step 8** From the **Schedule** area, select the radio button next to the day, week, or month for your scheduled report.

**Step 9** Select the language in which the report must be generated from the **Report Language** drop-down list.

**Step 10** Click **Submit**.

## Editing Scheduled Web Reports on the New Web Interface

To edit reports on the new web interface of your appliance, choose **Monitoring > Scheduled & Archive** page. Click on the link corresponding to the Report Title of report that you want to edit. Modify the settings and then click **Edit** to submit your changes on the page.

## Deleting Scheduled Web Reports on the New Web Interface

To delete reports on the new web interface of your appliance, choose **Monitoring > Scheduled / Archived** page. Select the checkboxes corresponding to the reports that you want to delete and click on the trash can icon.

To remove all scheduled reports, select the check box next to the report title. Note that archived versions of deleted reports are not deleted.

# Archiving Web Reports on the New Web Interface


- [New Web Interface] Generating Web Reports on Demand, on page 413
- Viewing and Managing Archived Web Reports on the New Web Interface, on page 414


## [New Web Interface] Generating Web Reports on Demand

Most reports that you can schedule, you can also generate on demand.

To generate a report on demand, perform the following:

### Procedure

**Step 1** On the Web Security Appliance , choose **Monitoring > Schedule & Archive**.

**Step 2** In the **View Archived** tab, click on the + button.

**Step 3** From the **Report Type** section, choose a report type from the drop-down list.

The options on the page may change.

**Step 4** In the **Report Title** section, enter the name of the title for the report.

AsyncOS does not verify the uniqueness of report names. To avoid confusion, do not create multiple reports with the same name.

**Step 5** From the **Time Range to Include** drop-down list, select a time range for the report data.

**Step 6** In the **Attachment Details** section, choose the format of the report.

PDF. Create a formatted PDF document for delivery, archival, or both. You can view the report as a PDF file immediately by clicking Preview PDF Report.

**Step 7** From the **Delivery Options** section, choose any one of the following:

By choosing this, the report will be listed on the Archived Reports page.

**Note**
Domain-Based Executive Summary reports cannot be archived.

- To archive the report, select **Only to Archive**.
- To archive and email the report, click **Archive and Email to Recipients**.
- To email the report, click **Only Email to Recipients**.

In the **Email IDs** field, enter the recipient email addresses.

**Step 8** Select the language in which the report must be generated from the **Report Language** drop-down list.

**Step 9** Click **Deliver This Report** to generate the report.

### Viewing and Managing Archived Web Reports on the New Web Interface

Use the information in this section to work with reports that are generated as scheduled reports.

### Procedure

**Step 1** Login to the new web interface of your appliance.

**Step 2** Select **Monitoring > Schedule& Archive**.

**Step 3** Select the **View Archived** tab.

**Step 4** To view a report, click the report names in the **Report Title** column. The Report Type drop-down list filters the types of reports that are listed on the **Archived Reports** tab.

**Step 5** You can search for a particular report in the search box.

# System Status Page on the New Web Interface

On the Web Security Appliance , choose **Monitoring > System Status** to monitor the System Status. This page displays the current status and configuration of the Web Security Appliance . Browser time is displayed on the system status page at the top right corner.

The **System Status** page has the following tabs:

The **Status** tab is displayed by default.

# Status

The Status page displays the following information.

| This Section... | Description |
|---|---|
| Web Security Appliance Status | • System uptime<br>• System resource utilization — CPU usage, RAM usage, and percentage of disk space used for reporting and logging.<br><br>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.<br><br>**Note**<br>Proxy Buffer Memory is one component that uses this RAM. |
| Alerts | Displays the alert names and the date and time at which it has occurred. When you click **More** at the top right corner or an alert name, the **All Alerts** pop-up appears. The selected alert row is highlighted in the **All Alerts** pop-up.<br><br>The **All Alerts** pop-up displays:<br>• Date and Time of Alert<br>• Alert Level - Info, Warning, or Critical<br>• Alert Class<br>• Problem - Short description of the alert<br>• Recipient - email address to which the alert details are sent |
| Disk Usage | Displays the value of disk usage and RAID storage status.<br><br>The RAID storage status depends on the appliance configuration. For virtual appliances, the RAID storage status displays "Unknown" and for physical appliances, it displays "Optimal". |
| Proxy Status | Displays Proxy CPU usage and Proxy Disk I/O utilization.<br><br>It also displays the proxy connection backlog with the port number and number of connections. |
| High Availability | Displays the Failover group name, Priority and Status.<br><br>It also displays the number of High Availability Failover groups enabled. If there are no failover groups, the service status displays "Not Configured". |

| This Section... | Description |
|---|---|
| Proxy Traffic Characteristics | Displays the following proxy traffic characteristics:<br>• Request Per Second<br>• Bandwidth<br>• Response Time<br>• Cache Hit Rate<br>It displays the average and maximum values of these data. The average values are shown for the last minute, last hour and since the proxy restart. The maximum values are shown for the last hour and since proxy restart. |

# Services

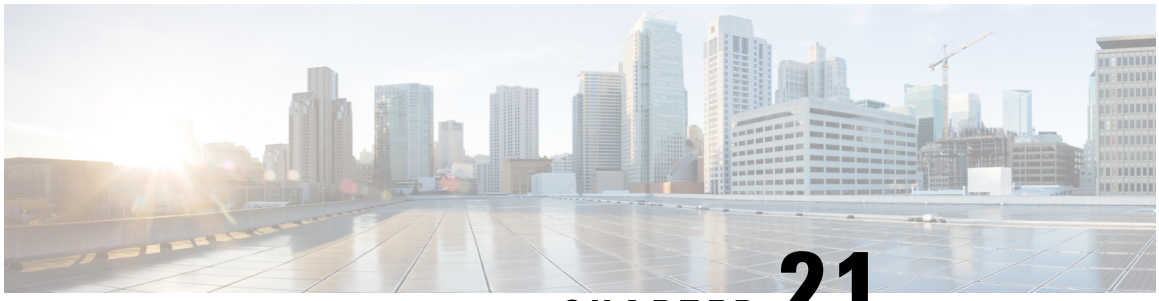
The Services page displays the services and its status. The services ribbon displays the status of AMP, WCCP, ISE, and CTR services. The color next to the service name denotes the service status:

- Red - The service is not ready.
- Grey - The service is ready, but disabled.
- Green - The service is ready, enabled and running.

| This Section... | Description |
|---|---|
| Date | The service data for the current day is displayed by default. You can view up to previous seven days data. Choose a date from the calendar to view the data for the particular day. |

| This Section... | Description |
|---|---|
| Service Status | The Service Status table displays the events and alerts for the services. The table displays a 24-hour time interval, which is divided into 1-hour slots. Each block represents the alerts in a 1-hour time interval.<br><br>Green color for a block indicates that there are no critical alerts in the corresponding hour. If there is at least one critical alert in an hour, the corresponding block appears in Red color. The blocks corresponding to future time slots is displayed in White.<br><br>The icon at the left side near the service name displays the color of the last block (or ongoing hour).<br><br>You can click the Red block to see the times at which the last 5 alerts have occurred. It also displays the total number of alerts as *5 of 'n' Events*, where '*n*' is the total number of alerts occurred during that time period. Click **More** to see the **All Alerts** pop-up.<br><br>The **All Alerts** pop-up displays:<br>• Date and Time of Alert<br>• Alert Level - Info, Warning, or Critical<br>• Alert Class<br>• Problem - Short description of the alert<br>• Recipient - email address to which the alert details are sent |

| This Section... | Description |
|---|---|
| Service Response Time | The Service Response Time table shows the response time pattern taken by each service running in the system. The following times are shown:<br>• McAfee Service Time<br>• WBRS Service Time<br>• DNS Response Time<br>• Webroot Service Time<br>• AMP Service Time<br>• Sophos Service Time<br>• Server Response Time<br>The table displays a 24-hour time interval divided into 1-hour slots. Each block represents the service response pattern in a 1-hour time. The response time for each service is split into the following time slots:<br>• 0.001s to 0.06s<br>• 0.06s to 0.6s<br>• 0.6s to 1s<br>• 1s to 6s<br>• 6s and more<br>By default, the table displays the 1s to 6s response values for all services. You can expand and view the detailed split up.<br>The system calculates the response time for all transactions. It then displays the percentage of transaction volume that has occurred in each timeslot. The block color is based on the transaction volume percentage. |



CHAPTER 21

# Detecting Rogue Traffic on Non-Standard Ports

This topic contains the following sections:


- Overview of Detecting Rogue Traffic, on page 419
- Configuring the L4 Traffic Monitor, on page 419
- List of Known Sites, on page 420
- Configuring L4 Traffic Monitor Global Settings, on page 420
- Updating L4 Traffic Monitor Anti-Malware Rules, on page 421
- Creating a Policy to Detect Rogue Traffic, on page 421
- Viewing L4 Traffic Monitor Activity, on page 422


## 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

**Procedure**

**Step 1** Configure the L4 Traffic Monitor inside the firewall.

**Step 2** 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 3** Configure the Global Settings

See Configuring L4 Traffic Monitor Global Settings, on page 420.

**Step 4** Create L4 TrafficMonitor Policies

See Creating a Policy to Detect Rogue Traffic, on page 421.

# 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 "allowed list" 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:<br>• Any *IP address* that is associated with both an unlisted *hostname* and a known malware *hostname* .<br>• Any *IP address* that is associated with both an unlisted *hostname* and a *hostname* from the Additional Suspected Malware Addresses property |
| **Known malware** | These appear in the log files as "blocked list" addresses and include:<br>• Any IP address or hostname that the L4 Traffic Monitor Database determines to be a known malware site and *not* listed in the Allow List.<br>• Any *IP address* that is listed in the Additional Suspected Malware Addresses property, *not* listed in the Allow List and is *not* ambiguous |

# Configuring L4 Traffic Monitor Global Settings

### Procedure

**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

**Procedure**

**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 :

**Procedure**

**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:<br>• 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.<br>• 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.

- 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.

- In a VM setup, the requests in transparent mode are duplicated while passing through the P1 and T1 interfaces at an intermittent time difference. Hence, some IPs even after blocking them may pass through the appliance.

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.

### What to do next

### Related Topics

- Overview of Detecting Rogue Traffic, on page 419
- Valid Formats, on page 422.

## 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 |

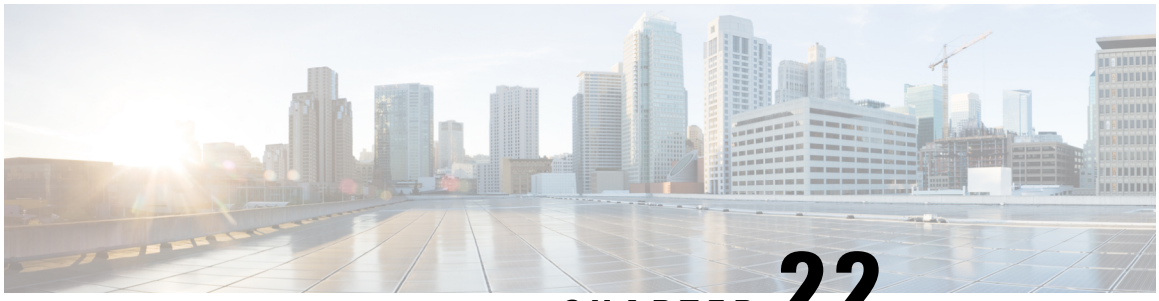
| To view... | See... |
|---|---|
| Malware statistics<br>Port statistics | Reporting > L4 Traffic Monitor |
| L4 Traffic Monitor log files | System Administration > Log Subscriptions<br>• trafmon_errlogs<br>• trafmonlogs |



**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.



CHAPTER 22

# Monitor System Activity Through Logs

This topic contains the following sections:


- Overview of Logging, on page 425
- Common Tasks for Logging, on page 426
- Best Practices for Logging, on page 426
- Troubleshooting Web Proxy Issues Using Logs, on page 426
- Log File Types, on page 427
- Adding and Editing Log Subscriptions, on page 432
- Pushing Log Files to Another Server, on page 437
- Archiving Log Files, on page 438
- Log File Names and Appliance Directory Structure, on page 439
- Viewing Log Files, on page 440
- Web Proxy Information in Access Log Files, on page 440
- W3C Compliant Access Log Files, on page 458
- Customizing Access Logs, on page 460
- Traffic Monitor Log Files, on page 464
- Log File Fields and Tags, on page 465
- Troubleshooting Logging, on page 478


## 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 types 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.

### Related Topics

- Common Tasks for Logging, on page 426
- Log File Types, on page 427

# Common Tasks for Logging

| Task | Links to Related Topics and Procedures |
|---|---|
| Add and edit log subscriptions | Adding and Editing Log Subscriptions, on page 432 |
| View log files | Viewing Log Files, on page 440 |
| Interpret log files | Interpreting Access Log Scanning Verdict Entries, on page 451 |
| Customize log files | Customizing Access Logs, on page 460 |
| Push log files to another server | Pushing Log Files to Another Server, on page 437 |
| Archiving log files | Archiving Log Files, on page 438 |

# Best Practices for Logging

- Minimizing the number of log subscriptions will benefit system performance.
- Logging fewer details will benefit system performance.

# 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.

### Procedure

**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.

### What to do next

### Related Topics

- Log File Types, on page 427
- Adding and Editing Log Subscriptions, on page 432

# Log File Types

Some log types related to the web proxy component are not enabled. 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 can manually enable as required.

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.)<br>See also Log Files , on page 299. | Yes | Yes |

| Log File Type | Description | Supports Syslog Push? | Enabled by Default? |
|---|---|---|---|
| Audit Logs | Records AAA (Authentication, Authorization, and Accounting) events. Records all user interaction with the application and command-line interfaces, and captures committed changes.<br>Some of the audit log details are as follows:<br>• User - Logon<br>• User - Logon failed incorrect password<br>• User - Logon failed unknown user name<br>• User - Logon failed account expired<br>• User - Logoff<br>• User - Lockout<br>• User - Activated<br>• User - Password change<br>• User - Password reset<br>• User - Security settings/profile change<br>• User - Created<br>• User - Deleted/modified<br>• Group/Role - Deletion / modified<br>• Group /Role - Permissions change | 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 |
| 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 |

| Log File Type | Description | Supports Syslog Push? | Enabled by Default? |
|---|---|---|---|
| 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<br>(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<br>(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.<br>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.<br>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<br>(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 |
| Haystack Logs | Haystack logs record web transaction tracking data processing. | Yes | Yes |

| Log File Type | Description | Supports Syslog Push? | Enabled by Default? |
|---|---|---|---|
| HTTPS Logs | Records Web Proxy messages specific to the HTTPS Proxy (when the HTTPS Proxy is enabled). | No | No |
| ISE Server Logs | Records ISE server(s) connection and operational information. | Yes | Yes |
| 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<br>(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 |

| Log File Type | Description | Supports Syslog Push? | Enabled by Default? |
|---|---|---|---|
| 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.<br>**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 |
| SHD Logs<br>(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<br>(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 |

| Log File Type | Description | Supports Syslog Push? | Enabled by Default? |
|---|---|---|---|
| W3C Logs | Records Web Proxy client history in a W3C compliant format.<br>For more information, see W3C Compliant Access Log Files, on page 458. | Yes | No |
| WBNP Logs<br>(SensorBase Network Participation) | Records a history of Cisco SensorBase Network participation uploads to the SensorBase network. | No | Yes |
| WBRS Framework Logs<br>(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 |
| 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 |

# Adding and Editing Log Subscriptions

You can create multiple log subscriptions for each type of log file. Subscriptions include configuration details for archiving and storage, including these:

- Rollover settings, which determine when log files are archived.
- Compression settings for archived logs.
- Retrieval settings for archived logs, which specifies whether logs are archived onto a remote server or stored on the appliance.

## Procedure

**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** Configure the subscription:

| Option | Description |
|---|---|
| Log Type | 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.<br>**Note**<br>The Request Debug Logs log type can only be subscribed to using the CLI and does not appear on this list. |
| 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. Enter only ASCII characters ([0-9], [A-Z], [a-z], and_). |
| 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. Enter a number between 100 kilobytes and 10 gigabytes. |
| Rollover by Time | The maximum time interval before the current log file is archived and a new log file started. The following interval types are available:<br>• **None.** AsyncOS only performs a rollover when the log file reaches the maximum file size.<br>• **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 d , h , m , and s as suffixes.<br>• **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.<br>• **Weekly Rollover.** AsyncOS performs a rollover on one or more days of the week at a specified time. |
| Log Style<br>(Access Logs) | Specifies the log format to use, either Squid, Apache, or Squid Details. |

| Option | Description |
|---|---|
| Custom Fields<br>(Access Logs) | Allows you to include custom information in each access log entry.<br>The syntax for entering format specifiers in the Custom Field is as follows:<br>`<format_specifier_1> <format_specifier_2> ...`<br>For example: `%a %b %E`<br>You can add tokens before the format specifiers to display descriptive text in the access log file. For example:<br>`client_IP %a body_bytes %b error_type %E`<br>where `client_IP` is the description token for log format specifier `%a`, and so on. |
| File Name | The name of the log files. Current log files are appended with a `.c` extension and rolled over log files are appended with the file creation timestamp and a `.s` extension. |
| Log Fields<br>(W3C Access Logs) | Allows you to choose the fields you want to include in the W3C access log.<br>Select a field in the Available Fields list, or type a field in the Custom Field box, and click Add.<br>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**.<br>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**.<br>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<br>You can anonymize the *c-ip*, *cs-username*, or *cs-auth-group* log fields of W3C logs, if required. Check the **Anonymization** check box to anonymize *c-ip*, *cs-username*, and *cs-auth-group* fields. After you select the check box, the field names are changed to *c-a-ip*, *cs-a-username,* and *cs-a-auth-group* respectively.<br>**Note**<br>You must enable anonymization only if the external server to which the log files are pushed is compatible to handle the anonymization feature.<br>After the log creation you can deanonymize the anonymized fields, if required. See Deanonymizing W3C Log Fields, on page 437 |
| Passphrase for Anonymization<br>(W3C Access Logs) | Allows you to create passphrase for encrypting the field values. This area will be enabled only when you choose to anonymize *c-ip*, *cs-username*, or *cs-auth-group* log fields.<br>**Note**<br>Sytem applies passphrase rules while configuring passphrase for anonymization.<br>To automatically generate a passphrase, check the check box next to **Auto Generate Passphrase** and click **Generate**<br>**Note**<br>If you have multiple appliances, all the appliances must set the same passphrase. |

| Option | Description |
|---|---|
| Log Compression | Specifies whether or not rolled over files are compressed. AsyncOS compresses log files using the gzip compression format. |
| Log Exclusions (Optional)<br>(Access Logs) | 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.<br>For example, entering 401 will filter out authentication failure requests that have that transaction number. |
| Log Level | Specifies the level of detail for log entries. Choose from:<br>• **Critical**. Includes errors only. This is the least detailed setting and is equivalent to the syslog level "Alert."<br>• **Warning**. Includes errors and warnings. This log level is equivalent to the syslog level "Warning."<br>• **Information**. Includes errors, warnings and additional system operations. This is the default detail level and is equivalent to the syslog level "Info."<br>• **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."<br>• **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."<br>**Note**<br>More detailed settings create larger log files and have a greater impact on system performance. |
| Retrieval Method | Specifies where rolled over log files are stored and how they are retrieved for reading. See below for descriptions of the available methods. |
| Retrieval Method:<br>FTP on Appliance | 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 passphrase.<br>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.<br>This is the default retrieval method. |

| Option | Description |
|---|---|
| Retrieval Method:<br>FTP on Remote Server | The FTP on Remote Server method (equivalent to FTP Push) periodically pushes log files to an FTP server on a remote computer.<br>When you choose this method, you must enter the following information:<br>• FTP server hostname<br>• Directory on FTP server to store the log file<br>• Username and passphrase of a user that has permission to connect to the FTP server<br>**Note**<br>AsyncOS for Web only supports passive mode for remote FTP servers. It cannot push log files to an FTP server in active mode. |
| Retrieval Method:<br>SCP on Remote Server | 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.<br>When you choose this method, you must enter the following information:<br>• SCP server hostname<br>• Directory on SCP server to store the log file<br>• Username of a user that has permission to connect to the SCP server<br>**Note**<br>Currently, we support only SSH-RSA and SSH-DSS in non-FIPS mode as well as SSH-RSA in FIPS mode. |
| Retrieval Method:<br>Syslog Push | You can only choose syslog for text-based logs.<br>The Syslog Push method sends log messages to a remote syslog server on port 514. This method conforms to RFC 3164.<br>When you choose this method, you must enter the following information:<br>• Syslog server hostname<br>• Protocol to use for transmission, either UDP or TCP<br>• Maximum message size<br>Valid values for UDP are 1024 to 9216.<br>Valid values for TCP are 1024 to 65535.<br>Maximum message size depends on the syslog server configuration.<br>• Facility to use with the log |

**Step 4** Submit and commit your changes.

### What to do next

If you chose SCP as the retrieval method, notice that the appliance displays an SSH key, which you will add to the SCP server host. See Pushing Log Files to Another Server, on page 437.

**Related Topics**

- Log File Types, on page 427
- Log File Names and Appliance Directory Structure, on page 439

# Deanonymizing W3C Log Fields

If you have enabled anonymization feature for field values (*c-ip, cs-username,* and *cs-auth-group*) during log subscription, the destination log server will receive the anonymized values ( *c-a-ip*, *cs-a-username*, and *cs-a-auth-group*) of those log fields and not the actual values. If you want to view the actual values you must deanonymize the log fields.

You can deanonymize *c-a-ip*, *cs-a-username*, and *cs-a-auth-group* log field values that are anonymized while adding the W3C log subscription.

### Procedure

**Step 1** Choose **System Administration** > **Log Subscriptions**.

**Step 2** Click **Deanonymization** in the Denonymization column corresponding to the log for which you want to deanonymize the anonymized fields.

**Step 3** In the **Method** area, choose any of the following methods to enter the encrypted text for deanonymization.

- Paste encrypted text – Paste only the encrypted text in the Anonymized Text field. You can enter a maximum of 500 entries in this field. You must separate the multiple entries with a comma.
- Upload File –Choose a file that contains the encrypted text. The file can contain a maximum of 1000 entries. The file format should be CSV. The system supports space, new line, tab, and semi colon as the field separator.

**Note**
If you have changed the passphrase, you must enter the old passphrase to deanonymize the older data.

**Step 4** Click **Deanonymize** and the Deanonymization Result table displays the deanonymized log field values.

# Pushing Log Files to Another Server

### Before you begin

Create or edit the desired log subscription, choosing SCP as the retrieval method. Adding and Editing Log Subscriptions, on page 432

**Procedure**

**Step 1** Add keys to the remote system:

a) Access the CLI.

b) Enter the `logconfig -> hostkeyconfig` command.

c) Use the commands below to display the keys:

| Command | Description |
|---|---|
| Host | Display system host keys. This is the value to place in the remote system's 'known_hosts' file. |
| 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. |

d) Add these keys to the remote system.

**Step 2** Still in the CLI, add the remote server's SSH public host key to the appliance:

| Command | Description |
|---|---|
| New | Add a new key. |
| Fingerprint | Display system host key fingerprints. |

**Step 3** Commit your changes.

# Archiving Log Files

AsyncOS archives (rolls over) log subscriptions when a current log file reaches a user-specified limit of maximum file size or maximum time since last rollover.

These archive settings are included in log subscriptions:

- Rollover by File Size
- Rollover by Time
- Log Compression
- Retrieval Method

You can also manually archive (rollover) log files.

**Procedure**

**Step 1** Choose **System Administration > Log Subscriptions**.

**Step 2** Check the checkbox in the Rollover column of the log subscriptions you wish to archive, or check the **All** checkbox to select all the subscriptions.

**Step 3** Click **Rollover Now** to archive the selected logs.

### What to do next

**Related Topics**

- Adding and Editing Log Subscriptions, on page 432
- Log File Names and Appliance Directory Structure, on page 439

# 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.

# 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, on page 440.
- Web Proxy Information in Access Log Files, on page 440.
- Interpreting W3C Access Logs, on page 458.
- Interpreting Traffic Monitor Logs, on page 464.
- Log File Fields and Tags, on page 465.

# Viewing Log Files

### Before you begin

Be aware that this method of viewing is for log files that are stored on the appliance. The process of viewing files stored externally goes beyond the scope of this documentation.

### Procedure

**Step 1** Choose **System 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 administers username and passphrase 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.

**Step 5** Refresh the browser for updated results.

**Note**
If a log subscription is compressed, download, decompress, and then open it.

### What to do next

**Related Topics**

- Web Proxy Information in Access Log Files, on page 440.
- Interpreting W3C Access Logs, on page 458.
- Interpreting Traffic Monitor Logs, on page 464.

# Web Proxy Information in 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.

Access logs are available in two formats: Standard and W3C compliant. W3C-compliant log files are more customizable with regard to their content and layout than standard Access logs.

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-PolicyGroupName-Identity-
OutboundMalwareScanningPolicy-DataSecurityPolicy-ExternalDLPPolicy-RoutingPolicy-NONE
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","""-",-,-,IW_comp,-,"-","-",
"Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,
"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e”>
 -
```

| Format Specifier | Field Value | Field Description |
|---|---|---|
| %t | `1278096903.150` | Timestamp since UNIX epoch. |
| %e | `97` | Elapsed time (latency) in milliseconds. |
| %a | `172.xx.xx.xx` | Client IP address.<br>**Note:** You can choose to mask the IP address in the access logs using the advancedproxyconfig > authentication CLI command. |
| %w | `TCP_MISS` | Transaction result code.<br>For more information, see W3C Compliant Access Log Files, on page 458. |
| %h | `200` | HTTP response code. |
| %s | `8187` | Response size (headers + body). |
| %1r<br>%2r | `GET http://my.site.com/` | First line of the request.<br>Note: When the first line of the request is for a native FTP transaction, some special characters in the file name are URL encoded in the access logs. For example, the "@" symbol is written as "%40" in the access logs.<br>The following characters are URL encoded:<br>& # % + , : ; = @ ^ { } [ ] |
| %A | – | Authenticated username.<br>**Note:** You can choose to mask the username in the access logs using the `advancedproxyconfig` > `authentication` CLI command. |

| Format Specifier | Field Value | Field Description |
|---|---|---|
| %H | `DIRECT` | Code that describes which server was contacted for the retrieving the request content.<br>Most common values include:<br>• **NONE.** The Web Proxy had the content, so it did not contact any other server to retrieve the content.<br>• **DIRECT.** The Web Proxy went to the server named in the request to get the content.<br>• **DEFAULT_PARENT.** The Web Proxy went to its primary parent proxy or an external DLP server to get the content. |
| %d | `my.site.com` | Data source or server IP address. |
| %c | `text/plain` | Response body MIME type. |
| %D | `DEFAULT_CASE_11` | ACL decision tag.<br>**Note:** The end of the ACL decision tag includes a dynamically generated number that the Web Proxy uses internally. You can ignore this number.<br>For more information, see ACL Decision Tags, on page 445. |
| N/A (Part of the ACL decision tag) | `PolicyGroupName` | Name of policy group responsible for the final decision on this transaction (Access Policy, Decryption Policy, or Data Security Policy). When the transaction matches a global policy, this value is "DefaultGroup."<br>Any space in the policy group name is replaced with an underscore ( _ ). |
| N/A (Part of the ACL decision tag) | `Identity` | Identity policy group name.<br>Any space in the policy group name is replaced with an underscore ( _ ). |

| Format Specifier | Field Value | Field Description |
|---|---|---|
| N/A (Part of the ACL decision tag) | `OutboundMalwareScanningPolicy` | Outbound Malware Scanning Policy group name.<br>Any space in the policy group name is replaced with an underscore ( _ ). |
| N/A (Part of the ACL decision tag) | `DataSecurityPolicy` | Cisco Data Security Policy group name. When the transaction matches the global Cisco Data Security Policy, this value is “DefaultGroup.” This policy group name only appears when Cisco Data Security Filters is enabled. “NONE” appears when no Data Security Policy was applied.<br>Any space in the policy group name is replaced with an underscore ( _ ). |
| N/A (Part of the ACL decision tag) | `ExternalDLPPolicy` | External DLP Policy group name. When the transaction matches the global External DLP Policy, this value is “DefaultGroup.” “NONE” appears when no External DLP Policy was applied.<br>Any space in the policy group name is replaced with an underscore ( _ ). |
| N/A (Part of the ACL decision tag) | `RoutingPolicy` | Routing Policy group name as *ProxyGroupName/ProxyServerName* .<br>When the transaction matches the global Routing Policy, this value is “DefaultRouting.” When no upstream proxy server is used, this value is “DIRECT.”<br>Any space in the policy group name is replaced with an underscore ( _ ). |

| Format Specifier | Field Value | Field Description |
|---|---|---|
| %Xr | <IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,""-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"> | Scanning verdict information. Inside the angled brackets, the access logs include verdict information from various scanning engines.<br>**Note**<br>In AsyncOS version 11.8 and later, the URL category identifier appears in double quotes. For example, "IW_comp".<br><br>For more information about the values included within the angled brackets, see Interpreting Access Log Scanning Verdict Entries, on page 451 and Malware Scanning Verdict Values, on page 477. |
| %?BLOCK_SUSPECT_USER_AGENT, MONITOR_SUSPECT_USER_AGENT?% < User-Agent:%!%-% | – | Suspect user agent. |

# 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 |
|---|---|
| `TCP_HIT` | The object requested was fetched from the disk cache. |
| `TCP_IMS_HIT` | 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. |
| `TCP_MEM_HIT` | The object requested was fetched from the memory cache. |
| `TCP_MISS` | The object was not found in the cache, so it was fetched from the origin server. |
| `TCP_REFRESH_HIT` | 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. |

| Result Code | Description |
|---|---|
| TCP_CLIENT_REFRESH_MISS | 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. |
| TCP_DENIED | The client request was denied due to Access Policies. |
| UDP_MISS | The object was fetched from the origin server. |
| NONE | There was an error in the transaction. For example, a DNS failure or gateway timeout. |

# 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_REFERER | The Web Proxy allowed the transaction based on an embedded/referred content exemption. |
| ALLOW_WBRS | The Web Proxy allowed the transaction based on the Web Reputation filter settings for the Access Policy group. |
| AMP_FILE_VERDICT | Value representing a verdict from the AMP reputation server for the file:<br>• 1 – Unknown<br>• 2 – Clean<br>• 3 – Malicious<br>• 4 – Unscannable |

| ACL Decision Tag | Description |
|---|---|
| ARCHIVESCAN_ALLCLEAR<br>ARCHIVESCAN_BLOCKEDFILETYPE<br>ARCHIVESCAN_NESTEDTOODEEP<br>ARCHIVESCAN_UNKNOWNFMT<br>ARCHIVESCAN_UNSCANABLE<br>ARCHIVESCAN_FILETOOBIG | **Archive scan Verdict**<br>ARCHIVESCAN_ALLCLEAR – There are no blocked file types in the inspected archive.<br>ARCHIVESCAN_BLOCKEDFILETYPE – There is a blocked file type in the inspected archive. The next field in the log entry (Verdict Detail) provides details, specifically the type of file blocked, and the name of the blocked file.<br>ARCHIVESCAN_NESTEDTOODEEP – The archive is blocked because it contains more "encapsulated" or nested archives than the configured maximum. The Verdict Detail field contains "UnScanable Archive-Blocked."<br>ARCHIVESCAN_UNKNOWNFMT – The archive is blocked because it contains a file type of unknown format. The Verdict Detail is "UnScanable Archive-Blocked."<br>ARCHIVESCAN_UNSCANABLE – The archive is blocked because it contain a file which cannot be scanned. The Verdict Detail is "UnScanable Archive-Blocked."<br>ARCHIVESCAN_FILETOOBIG – The archive is blocked because the size of the archive is more than the configured maximum. The Verdict Detail is "UnScanable Archive-Blocked."<br>**Archive scan Verdict Detail**<br>The field following the Verdict field in the log entry provides additional information about the Verdict, such as type of file blocked and name of the blocked file, "UnScanable Archive-Blocked," or "-" to indicate the archive does not contain any blocked file types.<br>For example, if an Inspectable Archive file is blocked (ARCHIVESCAN_BLOCKEDFILETYPE) based on Access Policy: Custom Objects Blocking settings, the Verdict Detail entry includes the type of file blocked, and the name of the blocked file.<br>Refer to Access Policies: Blocking Objects, on page 226 and Archive Inspection Settings, on page 229 for more information about Archive Inspection. |
| BLOCK_ADC | Transaction blocked based on the configured Application settings for the Access Policy group. |
| BLOCK_ADMIN | Transaction blocked based on some default settings for the Access Policy group. |
| BLOCK_ADMIN_CONNECT | Transaction blocked 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 | Transaction blocked based on the user agent as defined in the Block Custom User Agents setting for the Access Policy group. |

| ACL Decision Tag | Description |
|---|---|
| BLOCK_ADMIN_TUNNELING | The Web Proxy blocked the transaction based on tunneling of the non HTTP traffic on the HTTP ports for the Access Policy Group. |
| BLOCK_ADMIN_HTTPS_ NonLocalDestination | Transaction blocked; client tried to bypass authentication using the SSL port as an explicit proxy. To prevent this, if an SSL connection is to the Web Security Appliance itself, only requests to the actual Web Security Appliance redirect hostname are allowed. |
| BLOCK_ADMIN_IDS | Transaction blocked based on the MIME type of the request body content as defined in the Data Security Policy group. |
| BLOCK_ADMIN_FILE_TYPE | Transaction blocked based on the file type as defined in the Access Policy group. |
| BLOCK_ADMIN_PROTOCOL | Transaction blocked based on the protocol as defined in the Block Protocols setting for the Access Policy group. |
| BLOCK_ADMIN_SIZE | Transaction blocked based on the size of the response as defined in the Object Size settings for the Access Policy group. |
| BLOCK_ADMIN_SIZE_IDS | Transaction blocked 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 | Transaction blocked based on the configured Application settings for the Access Policy group. |
| BLOCK_CONTENT_UNSAFE | Transaction blocked 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 | Transaction blocked 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 | Transaction blocked and displayed the Warn and Continue page based on a custom URL category in the Access Policy group configured to "Warn." |

| ACL Decision Tag | Description |
|---|---|
| BLOCK_CONTINUE_WEBCAT | Transaction blocked and displayed the Warn and Continue page based on a predefined URL category in the Access Policy group configured to “Warn.” |
| BLOCK_CUSTOMCAT | Transaction blocked 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 | Transaction blocked based on the Suspect User Agent setting for the Access Policy group. |
| BLOCK_UNSUPPORTED_SEARCH_APP | Transaction blocked 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 | Transaction blocked 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 | Transaction blocked 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. |
| BLOCK_YTCAT | The Web Proxy blocked the transaction based on the predefined YouTube category filtering settings for the Access Policy group. |
| BLOCK_CONTINUE_YTCAT | The Web Proxy blocked the transaction and displayed the Warn and Continue page based on a predefined YouTube category in the Access Policy group configured to 'Warn'. |
| DECRYPT_ADMIN | The Web Proxy decrypted the transaction based on some default settings for the Decryption Policy group. |
| DECRYPT_ADMIN_EXPIRED_CERT | The Web Proxy decrypted the transaction although the server certificate has expired. |
| DECRYPT_EUN_ADMIN_DEFAULT_ACTION | The Web Proxy decrypted the transaction based on default settings as drop connection for the decryption policy group when EUN is enabled. |
| DECRYPT_EUN_ADMIN_EXPIRED_CERT | The Web Proxy decrypted the transaction when HTTPS proxy settings drop an expired certificate with EUN enabled. |

| ACL Decision Tag | Description |
|---|---|
| DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT | The Web Proxy decrypted the transaction when HTTPS proxy settings drop an invalid leaf certificate with EUN enabled. |
| DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME | The Web Proxy decrypted the transaction when HTTPS proxy settings drop the mismatched hostname with EUN enabled. |
| DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR | The Web Proxy decrypted the transaction when HTTPS proxy settings drop an OCSP with other errors with EUN enabled. |
| DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT | The Web Proxy decrypted the transaction when HTTPS proxy settings drop an OCSP revoked certificate with EUN enabled. |
| DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT | The Web Proxy decrypted the transaction when HTTPS proxy settings drop an unrecognized root authority or issuer certificate with EUN enabled. |
| DECRYPT_EUN_CUSTOMCAT | The Web Proxy decrypted the transaction based on custom URL category filtering settings for the decryption policy group. If EUN is enabled, the traffic is dropped. |
| DECRYPT_EUN_WBRS | The Web Proxy decrypted the transaction based on the web reputation filter settings for the decryption policy group. If EUN is enabled, the traffic is dropped. |
| DECRYPT_EUN_WBRS_NO_SCORE | The Web Proxy decrypted the transaction based on the web reputation filter settings for no score URL in the decryption policy group. If EUN is enabled, the traffic is dropped. |
| DECRYPT_EUN_WEBCAT | The Web Proxy decrypted the transaction based on URL category filtering settings for the decryption policy group. If EUN is enabled, the traffic is dropped. |
| 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. |
| 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. |
| DENY_ADMIN | The Web Proxy denied the transaction. This occurs for HTTPS requests when authentication is required and 'Decrypt for Authentication' is disabled in the HTTPS proxy settings. |
| DROP_ADMIN | The Web Proxy dropped the transaction based on some default settings for the Decryption Policy group. |
| DROP_ADMIN_EXPIRED_CERT | The Web Proxy dropped the transaction because the server certificate has expired. |

| ACL Decision Tag | Description |
|---|---|
| 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_ADC | The Web Proxy monitored the transaction based on the Application settings for the Access Policy group. |
| MONITOR_ADMIN_EXPIRED_CERT | The Web Proxy monitored the server response because the server certificate has expired. |
| 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_CONTINUE_YTCAT | Originally, the Web Proxy blocked the transaction and displayed the Warn and Continue page based on a predefined YouTube 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. |

| ACL Decision Tag | Description |
|---|---|
| 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. |
| 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_ADMIN_EXPIRED_CERT | The Web Proxy passed through the transaction although the server certificate has expired. |
| 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. |

# 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",

ARCHIVESCAN_BLOCKEDFILETYPE,

EXT_ARCHIVESCAN_VERDICT,

EXT_ARCHIVESCAN_THREATDETAIL,

EXT_WTT_BEHAVIOR,
EXT_YTCAT,
"BlockedFileType: application/x-rpm,
BlockedFile: allfiles/linuxpackage.rp">
```

**Note** For an example of a whole access log file entry, see Web Proxy Information in Access Log Files, on page 440.

Each element in this example corresponds to a log-file format specifier as shown in the following table:

| Position | Field Value | Format Specifier | Description |
|---|---|---|---|
| 1 | `IW_infr` | %XC | The custom URL category assigned to the transaction, abbreviated. This field shows “nc” when no category is assigned. |
| 2 | `ns` | %XW | Web Reputation filters score. This field either shows the score as a number, “ns” for no score, or “dns” when there is a DNS lookup error. |
| 3 | `24` | %Xv | The malware scanning verdict Webroot passed to the DVS engine. Applies to responses detected by Webroot only.<br>For more information, see Malware Scanning Verdict Values, on page 477. |
| 4 | `“Trojan-Phisher-Gamec”` | “%Xn” | Name of the spyware that is associated with the object. Applies to responses detected by Webroot only. |
| 5 | `0` | %Xt | The Webroot specific value associated with the Threat Risk Ratio (TRR) value that determines the probability that malware exists. Applies to responses detected by Webroot only. |
| 6 | `354385` | %Xs | A value that Webroot uses as a threat identifier. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Webroot only. |

| Position | Field Value | Format Specifier | Description |
|---|---|---|---|
| 7 | 12559 | %Xi | A value that Webroot uses as a trace identifier. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Webroot only. |
| 8 | - | %Xd | The malware scanning verdict McAfee passed to the DVS engine. Applies to responses detected by McAfee only.<br>For more information, see Malware Scanning Verdict Values, on page 477. |
| 9 | "-" | "%Xe" | The name of the file McAfee scanned. Applies to responses detected by McAfee only. |
| 10 | - | %Xf | A value that McAfee uses as a scan error. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only. |
| 11 | - | %Xg | A value that McAfee uses as a detection type. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only. |
| 12 | - | %Xh | A value that McAfee uses as a virus type. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by McAfee only. |
| 13 | "-" | "%Xj" | The name of the virus that McAfee scanned. Applies to responses detected by McAfee only. |
| 14 | - | %XY | The malware scanning verdict Sophos passed to the DVS engine. Applies to responses detected by Sophos only.<br>For more information, see Malware Scanning Verdict Values, on page 477. |
| 15 | - | %Xx | A value that Sophos uses as a scan return code. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Sophos only. |
| 16 | "-" | "%Xy" | The name of the file in which Sophos found the objectionable content. Applies to responses detected by Sophos only. |

| Position | Field Value | Format Specifier | Description |
|---|---|---|---|
| 17 | "-" | "%Xz" | A value that Sophos uses as the threat name. Cisco Customer Support may use this value when troubleshooting an issue. Applies to responses detected by Sophos only. |
| 18 | - | %Xl | The Cisco Data Security scan verdict based on the action in the Content column of the Cisco Data Security Policy. The following list describes the possible values for this field:<br>• **0.** Allow<br>• **1.** Block<br>• **- (hyphen).** No scanning was initiated by the Cisco Data Security Filters. This value appears when the Cisco Data Security Filters are disabled, or when the URL category action is set to Allow. |
| 19 | - | %Xp | The External DLP scan verdict based on the result given in the ICAP response. The following list describes the possible values for this field:<br>• **0.** Allow<br>• **1.** Block<br>• **- (hyphen).** No scanning was initiated by the external DLP server. This value appears when External DLP scanning is disabled, or when the content was not scanned due to an exempt URL category on the External DLP Policies > Destinations page. |
| 20 | `IW_infr` | %XQ | The predefined URL category verdict determined during request-side scanning, abbreviated. This field lists a hyphen ( - ) when URL filtering is disabled.<br>**Note**<br>In AsyncOS version 11.8 and later, the URL category identifier appears in double quotes. For example, "IW_infr".<br>For a list of URL category abbreviations, see URL Category Descriptions, on page 198. |

| Position | Field Value | Format Specifier | Description |
|---|---|---|---|
| 21 | - | %XA | The URL category verdict determined by the Dynamic Content Analysis engine during response-side scanning, abbreviated. Applies to the Cisco Web Usage Controls URL filtering engine only. Only applies when the Dynamic Content Analysis engine is enabled and when no category is assigned at request time (a value of "nc" is listed in the request-side scanning verdict).<br>For a list of URL category abbreviations, see URL Category Descriptions, on page 198. |
| 22 | "Trojan Phisher" | "%XZ" | Unified response-side anti-malware scanning verdict that provides the malware category independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning. |
| 23 | "-" | "%Xk" | The Category Name or Threat Type is returned by the Web Reputation filters. The Category Name is returned when the Web Reputation is high and Threat Type returned when the reputation is low. |
| 24 | "-" | %X#10# | The URL which is encapsulated inside Google translate engine. If there is no encapsulated URL, the field value will be "-". |
| 25 | "Unknown" | "%XO" | The application name as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled. |
| 26 | "Unknown" | "%Xu" | The application type as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled. |
| 27 | "-" | "%Xb" | The application behavior as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled. |
| 28 | "-" | "%XS" | Safe browsing scanning verdict. This value indicates whether either the safe search or the site content ratings feature was applied to the transaction.<br>For a list of the possible values, see Logging Adult Content Access, on page 191. |
| 29 | 489.73 | %XB | The average bandwidth consumed serving the request, in Kb/sec. |

| Position | Field Value | Format Specifier | Description |
|---|---|---|---|
| 30 | `0` | %XT | A value that indicates whether the request was throttled due to bandwidth limit control settings, where “1” indicates the request was throttled, and “0” indicates it was not. |
| 31 | `[Local]` | %l | The type of user making the request, either “[Local]” or “[Remote].” Only applies when AnyConnect Secure Mobility is enabled. When it is not enabled, the value is a hyphen (-). |
| 32 | “-” | “%X3” | Unified request-side anti-malware scanning verdict independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to client request scanning when an Outbound Malware Scanning Policy applies. |
| 33 | “-” | “%X4” | The threat name assigned to the client request that was blocked or monitored due to an applicable Outbound Malware Scanning Policy.<br>This threat name is independent of which anti-malware scanning engines are enabled. |
| 34 | `37` | %X#1# | Verdict from Advanced Malware Protection file scanning:<br>• 0: File is not malicious<br>• 1: File was not scanned because of its file type<br>• 2: File scan timed out<br>• 3: Scan error<br>• Greater than 3: File is malicious |
| 35 | `"W32.CiscoTestVector"` | %X#2# | Threat name, as determined by Advanced Malware Protection file scanning; "-" indicates no threat. |

| Position | Field Value | Format Specifier | Description |
|---|---|---|---|
| 36 | 33 | %X#3# | 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.<br>For details, see information about the Threat Score and the reputation threshold in File Reputation Filtering and File Analysis, on page 281 .<br>. |
| 37 | 0 | %X#4# | Indicator of upload and analysis request:<br>"0" indicates that Advanced Malware Protection did not request upload of the file for analysis.<br>"1" indicates that Advanced Malware Protection did request upload of the file for analysis. |
| 38 | "WSA-INFECTED-FILE.pdf" | %X#5# | The name of the file being downloaded and analyzed. |
| 39 | "fd5ef49d4213e05f448 f11ed9c98253d85829614fba 368a421d14e64c426da5e" | %X#6# | The SHA-256 identifier for this file. |
| 40 | ARCHIVESCAN_BLOCKEDFILETYPE | %X#8# | Archive scan Verdict. |
| 41 | EXT_ARCHIVESCAN_VERDICT | %Xo | Archive scan Verdict Detail. If an Inspectable Archive file is blocked (ARCHIVESCAN_BLOCKEDFILETYPE) based on Access policy: Custom Objects Blocking settings, this Verdict Detail entry includes the type of file blocked, and the name of the blocked file. |
| 42 | EXT_ARCHIVESCAN_THREATDETAIL | %Xm | File verdict by Archive Scanner |
| 43 | EXT_WTT_BEHAVIOR | %XU | Web Tap Behavior. |
| 44 | EXT_YTCAT | %X#29# | The YouTube URL category assigned to the transaction, abbreviated. This field shows "nc" when no category is assigned. |

Refer to Log File Fields and Tags, on page 465 for a description of each format specifier's function.

### Related Topics

- Web Proxy Information in Access Log Files, on page 440
- Customizing Access Logs, on page 460

- W3C Compliant Access Log Files, on page 458
- Viewing Log Files, on page 440
- Log File Fields and Tags, on page 465


# W3C Compliant Access Log Files

The Web Security Appliance provides two different log types for recording Web Proxy transaction information: access logs and W3C-formatted access logs. The W3C access logs are World Wide Web Consortium (W3C) compliant, and record transaction history in the W3C Extended Log File (ELF) Format.


- W3C Field Types, on page 458
- Interpreting W3C Access Logs, on page 458


## 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, on page 458
- W3C Field Prefixes, on page 459


### 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

- Web Proxy Information in Access Log Files, on page 440.
- Customizing Access Logs, on page 460.
- Traffic Monitor Log Files, on page 464.
- Log File Fields and Tags, on page 465.
- Viewing Log Files, on page 440.

# 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, on page 465.
- For information on user defined fields, see Access Log User Defined Fields, on page 460.

# 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 | %<*ClientHeaderName* : | cs(*ClientHeaderName* ) |
| Header from the server | %<*ServerHeaderName* : | sc(*ServerHeaderName* ) |

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, on page 460.
- Customizing W3C Access Logs, on page 461.

# Customizing Regular Access Logs

### Procedure

**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.

### What to do next

### Related Topics

- Web Proxy Information in Access Log Files, on page 440.
- Log File Fields and Tags, on page 465.
- Access Log User Defined Fields, on page 460.

# Customizing W3C Access Logs

### Procedure

**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.

### What to do next

### Related Topics

- W3C Compliant Access Log Files, on page 458.
- Log File Fields and Tags, on page 465.

- Access Log User Defined Fields, on page 460.
- Configuring Cisco CTA-specific Custom W3C Logs, on page 462
- Configuring Cisco Cloudlock-specific Custom W3C Logs, on page 463


## Configuring Cisco CTA-specific Custom W3C Logs

You can configure your appliance to push Cognitive Threat Analytics (CTA)-specific custom W3C access logs to Cisco Cloud Web Security service for analysis and reporting. Cisco ScanCenter is the administration portal of Cloud Web Security (CWS). See https://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html

### Before you begin

Create a device account in Cisco ScanCenter for your appliance, selecting SCP (Secure Copy Protocol) as the automatic upload protocol. See the Proxy Device Uploads section of the Cisco ScanCenter Administrator (https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide.html)

Note the SCP host name and the generated user name for your appliance. The user name is case sensitive and unique for each device.

### Procedure

**Step 1** Choose **Security Services** > **Cisco Cognitive Threat Analytics**.

**Step 2** Click **Edit Settings**.

**Step 3** In the **Log Fields** area, add additional log fields, if required. See Adding and Editing Log Subscriptions, on page 432.

**Step 4** From the **Selected Log Fields**, check the check boxes next to *c-ip*, *cs-username* or *cs-auth-group* if you want to anonymize these fields individually.

Alternatively, you can check the **Anonymization** check box to anonymize these fields simultaneously. See Adding and Editing Log Subscriptions, on page 432.

**Step 5** In the **Retrieval Method** area, enter the username generated for your device in Cisco ScanCenter. The device user name is case sensitive and unique for each proxy device.

**Step 6** Modify the **Advanced Options** values, if required.

**Step 7** Click **Submit**.

The appliance generates public SSH keys and displays them on the Cisco Cognitive Threat Analytics page.

**Step 8** Copy one of the public SSH key to the clipboard.

**Step 9** Click the **View Cisco Cognitive Threat Analytics** portal link to switch to the Cisco ScanCenter portal, select the appropriate device account and then paste the public SSH key to the CTA Device Provisioning page. (See the *Proxy Device Uploads* section of the Cisco ScanCenter Administrator Guide).

Log files from your proxy device will be uploaded to the CTA system for analysis on successful authentication between your proxy device and CTA system.

**Step 10** Switch back to the appliance and commit your changes.

You can also add CTA W3C logs using **System Administration** > **Log Subscription**. Follow the instructions in Customizing W3C Access Logs, on page 461 to add a new W3C access log subscription with the following options:

- **W3C Logs** as log type
- **Cisco Cognitive Threat Analytics Subscription** as subscription
- **SCP** as file transfer type

See Adding and Editing Log Subscriptions, on page 432 to know more about custom fields.

**Note**
If you have already configured a CTA log subscription, you must change the log name to *cta_log* to list it on the Cisco Cognitive Threat Analytics page in the appliance.

After log creation, if you want to delete the CTA log, click **Disable** in the Cisco Cognitive Threat Analytics page. You can also delete the CTA log from the Log Subscriptions page (**System Administration** > **Log subscriptions**).

To deanonymize the anonymized CTA-specific W3C log fields, click **Deanonymize** in the Cisco Cognitive Threat Analytics page. See Deanonymizing W3C Log Fields, on page 437

You can also deanonymize the anonymized CTA-specific W3C log fields using **System Administration** > **Log Subscription**. See Deanonymizing W3C Log Fields, on page 437

## Configuring Cisco Cloudlock-specific Custom W3C Logs

Cisco Cloudlock is a cloud-native CASB and cloud cybersecurity platform that protects users, data, and applications across Software-as-a-Service, Platform-as-a-Service, and Infrastructure-as-a-Service. You can configure your appliance to push W3C access logs to Cisco's Cloudlock portal for analysis and reporting. These custom W3C logs provide better visibility into the SaaS usage of the customers.

### Before you begin

Create a device account in Cloudlock portal for your appliance, selecting SCP as the automatic upload protocol.

Logon to Cloudlock portal, access the online help and follow the instructions to create device account in the Cloudlock portal.

### Procedure

**Step 1** Choose **Security Services** > **Cisco Cloudlock**.

**Step 2** Click **Edit Settings**.

**Note**
The log fields are selected by default in the **Log Fields** area.You cannot add additional log fields other than the log fields selected by default. You should not change the order of the log fields displayed in the **Log Fields** area.

You cannot anonymize log fields (*c-ip, cs-username,* or *cs-auth-group*) of Cloudlock log files.

**Step 3** In the **Retrieval Method** area, enter the following information:

- Cloudlock server hostname and port number
- Directory on the Cloudlock server to store the log file

- Username of the user who has permission to connect to the Cloudlock server

**Step 4** Modify the **Advanced Options** values if required.

**Step 5** Click **Submit**.

The appliance generates public SSH keys and displays them on the Cisco Cloudlock page.

**Step 6** Copy one of the public SSH key to the clipboard.

**Step 7** Click the **View Cloudlock Portal** link to switch to the Cisco Cloudlock portal. Select the appropriate device account and then paste the public SSH key into the Cloudlock Setting page.

Log files from your proxy device will be uploaded to the Cloudlock system for analysis on successful authentication between your proxy device and Cloudlock system.

**Step 8** Switch back to the appliance and commit your changes.

You can also add Cloudlock W3C logs using **System Administration** > **Log Subscription**. Follow the instructions in Customizing W3C Access Logs, on page 461 to add a new W3C access log subscription with the following options:

- **W3C Logs** as log type
- **Cisco Cloudlock** as subscription
- **SCP** as file transfer type

See Adding and Editing Log Subscriptions, on page 432 to know more about custom fields.

**Note**
If you have already configured a Cloudlock log subscription, you must change the log name to **cloudlock_log** to list it on the Cisco Cloudlock page in the appliance.

After log creation, if you want to delete the Cloudlock log, click **Disable** in the Cisco Cloudlock page. You can also delete the Cloudlock log from the Log Subscriptions page (**System Administration** > **Log subscriptions**).

# 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, on page 440

# Log File Fields and Tags


- Access Log Format Specifiers and W3C Log File Fields, on page 465
- Transaction Result Codes, on page 444
- ACL Decision Tags, on page 445
- Malware Scanning Verdict Values, on page 477


## Access Log Format Specifiers 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.

To configure Access Logs to display these values, see Customizing Access Logs, on page 460 and information about custom fields in Adding and Editing Log Subscriptions, on page 432.

The following table describes these variables:

| Format Specifier in Access Logs | Log Field in W3C Logs | Description |
|---|---|---|
| %:<A | AclTime | To print the total amount of time taken by the Access Control List transaction. |
| %[ | x-spoofed-ip | Source IP address used in proxy IP spoofing. |
| %) | x-proxy-instance-id | Instance ID of proxy if High Performance Mode is enabled, otherwise it logs a hyphen. |

| Format Specifier in Access Logs | Log Field in W3C Logs | Description |
|---|---|---|
| %( | cs-domain-map | Resolved domain name which are resolved using domain map. |
| %X#11# | ext_auth_sgt | Custom field parameter for Secure Group Tags used in ISE integrations. |
| %$ | cipher information | Cipher information of both the legs in the transaction.(Client-proxy cipher info##proxy-server cipher info).The information in the below sequence - <ciphername>, <protocol version>, Kx=<key exchange>, Au=<authentication>, Enc=<symmetric encryption method>, Mac=<message authentication code> |
| %:<l | 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. |
| %:<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. |
| %:>l | 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. |

| Format Specifier in Access Logs | Log Field in W3C Logs | Description |
|---|---|---|
| %:>h | x-s2p-header-time | Wait-time for server header after first response byte |
| %:>g | | SSL server handshake latency information. |
| %o | - | Time quota consumed. |
| % O | - | Volume quota consumed. |
| %:>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. |
| %: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-p2c-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. |

| Format Specifier in Access Logs | Log Field in W3C Logs | Description |
|---|---|---|
| %: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. |
| %aBLOCK_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. |
| %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. |

| Format Specifier in Access Logs | Log Field in W3C Logs | Description |
|---|---|---|
| %e | x-elapsed-time | Elapsed time in milliseconds.<br>For TCP traffic, this is the time elapsed between the opening and closing of the HTTP connection.<br>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. |
| %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.<br>This field is used for troubleshooting policy/authentication issues to determine whether a user is matching the correct group or policy. |
| %G | | Human-readable timestamp. |
| %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 | Do not cache response code; DCF flags.<br>Response code descriptions:<br>• Response code based on client request:<br>• 1 = Request had “no-cache” header.<br>• 2 = Caching is not authorized for the request.<br>• 4 = Request is missing the 'Variant' header.<br>• 8 = Username or passphrase needed for user request.<br>• 20 = Response for specified HTTP method.<br>• Response code based on response received by the appliance:<br>• id="li_7443F05D141F4D9FB788FD416697DB65"> 40 = Response contains “Cache-Control: private” header.<br>• 80 = Response contains “Cache-Control: no-store” header.<br>• 100 = Response indicates that request was a query.<br>• 200 = Response has a small “Expires” value (expires soon).<br>• 400 = Response does not have “Last Modified” header.<br>• 1000 = Response expires immediately.<br>• 2000 = Response file is too big to cache.<br>• 20000 = New copy of file exists.<br>• 40000 = Response has bad/invalid values in “Vary” header.<br>• 80000 = Response requires setting of cookies.<br>• 100000 = Non-cacheable HTTP STATUS Code.<br>• 200000 = Object received by appliance was incomplete (based on size).<br>• 800000 = Response trailers indicate no caching.<br>• 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)<br>This value is used to determine a requestor when the IP address is flagged by an intrusion detection device on your network. Allows you to locate a client that visited an IP address that has been so flagged. |
| %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.<br>Enabling this field allows you to correlate logs to issues without having to calculate local time from epoch time for each log entry. |
| %m | cs-auth-mechanism | Used to troubleshoot authentication issues.<br>The authentication mechanism used on the transaction. Possible values are:<br>• **BASIC.** The user name was authenticated using the Basic authentication scheme.<br>• **NTLMSSP.** The user name was authenticated using the NTLMSSP authentication scheme.<br>• **NEGOTIATE.** The user name was authenticated using the Kerberos authentication scheme.<br>• **SSO_TUI.** The user name was obtained by matching the client IP address to an authenticated user name using transparent user identification.<br>• **SSO_ISE.** The user was authenticated by an ISE server. (Log shows GUEST if that is chosen as the fall-back mechanism for ISE authentication.)<br>• **SSO_ASA.** The user is a remote user and the user name was obtained from a Cisco ASA using the Secure Mobility.<br>• **FORM_AUTH.** The user entered authentication credentials in a form in the web browser when accessing a application.<br>• **GUEST.** The user failed authentication and instead was granted guest access. |
| %M | CMF | Cache miss flags: CMF flags. |

| Format Specifier in Access Logs | Log Field in W3C Logs | Description |
|---|---|---|
| %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 used. Possible values are:<br>• 0 = No protocol used<br>• 1 = HTTP<br>• 2 = HTTPS<br>• 3 = FTP over HTTP<br>• 4 = FTP<br>• 5 = SOCKS<br>• 6 = HTTP2 |
| %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.<br>**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. |
| %u | cs(User-Agent) | User agent. This field is written with double-quotes in the access logs.<br>This field helps determine if an application is failing authentication and/or requires different access permissions. |
| %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. |

| Format Specifier in Access Logs | Log Field in W3C Logs | Description |
|---|---|---|
| %X0 | x-resp-dvs-scanverdict | Unified response-side anti-malware scanning verdict that provides the *malware category number* independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning.<br>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 *malware threat name* independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning.<br>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 Adaptive Scanning blocked the transaction without invoke any anti-malware scanning engine. The possible values are:<br>• **1.** Transaction was blocked.<br>• **0.** Transaction was not blocked.<br>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. |
| %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 custom 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). |

| Format Specifier in Access Logs | Log Field in W3C Logs | Description |
|---|---|---|
| %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. |
| %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 predefined URL category verdict determined during request-side scanning, abbreviated. |
| %Xr | x-result-code | Scanning verdict information. |

| Format Specifier in Access Logs | Log Field in W3C Logs | Description |
|---|---|---|
| %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.<br>Indicates whether 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 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” checkbox 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 name of the file in which Sophos found the objectionable content. Applies to responses detected by Sophos only. |
| %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 *malware category* independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning.<br>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:<br>• 0: File is not malicious.<br>• 1: File was not scanned because of its file type.<br>• 2: File scan timed out.<br>• 3: Scan error.<br>• Greater than 3: File is malicious. |
| %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.<br>This score is used only if the cloud reputation service is unable to determine a clear verdict for the file.<br>For details, see information about the Threat Score and the reputation threshold in File Reputation Filtering and File Analysis, on page 281 |
| %X#4# | x-amp-upload | Indicator of upload and analysis request:<br>"0" indicates that Advanced Malware Protection did not request upload of the file for analysis.<br>"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. |
| %:e< | x-p2p-amp-svc-time | Wait-time to receive the verdict from the AMP scanning engine, including the time required for the Web Proxy to send the request. |
| %:e> | x-p2p-amp-wait-time | Wait-time to receive the response from the AMP scanning engine, after the Web Proxy sent the request. |
| N/A | x-hierarchy-origin | Code that describes which server was contacted for the retrieving the request content (for example, DIRECT/www.example.com). |

| Format Specifier in Access Logs | Log Field in W3C Logs | Description |
|---|---|---|
| N/A | x-resultcode-httpstatus | Result code and the HTTP response code, with a slash (/) in between. |
| N/A | x-archivescan-verdict | Display the verdict of Archive Inspection. |
| N/A | x-archivescan-verdict- reason | Details of the file blocked by Archive Scan. |
| %XU | N/A | Reserved for future. |

### Related Topics

- Web Proxy Information in Access Log Files, on page 440.
- Interpreting W3C Access Logs, on page 458.

# 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 list presents the different Malware Scanning Verdict Values and each corresponding malware category:

| Malware Scanning Verdict Value | Malware Category |
|---|---|
| - | Not Set |
| 0 | Unknown |
| 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 |

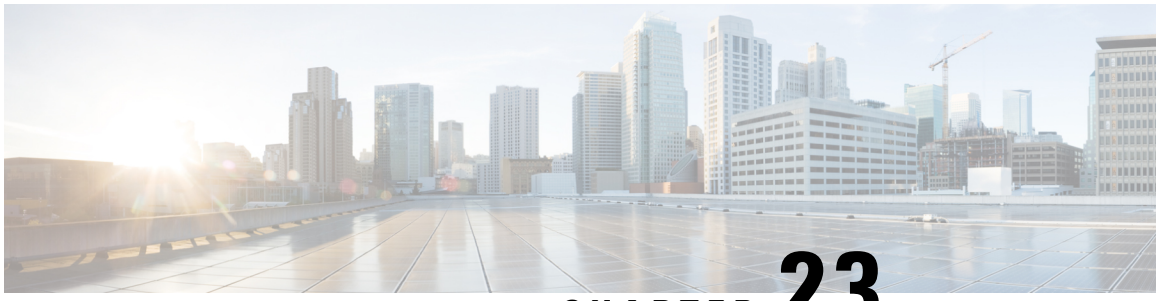
| Malware Scanning Verdict Value | Malware Category |
|---|---|
| 19 | Dialer |
| 20 | Hijacker |
| 21 | Phishing URL |
| 22 | Trojan Downloader |
| 23 | Trojan Horse |
| 24 | Trojan Phisher |
| 25 | Worm |
| 26 | Encrypted File |
| 27 | Virus |
| 33 | Other Malware |
| 34 | PUA |
| 35 | Aborted |
| 36 | Outbreak Heuristics |
| 37 | Known Malicious and High-Risk Files |

### Related Topics

- Web Proxy Information in Access Log Files, on page 440.
- Interpreting W3C Access Logs, on page 458.

# Troubleshooting Logging


- Custom URL Categories Not Appearing in Access Log Entries, on page 570
- Logging HTTPS Transactions, on page 570
- Alert: Unable to Maintain the Rate of Data Being Generated, on page 570
- Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs, on page 571



CHAPTER 23

# Integrating with Cisco Threat Response

This topic contains the following sections:


- Integrating the Appliance with Cisco Threat Response, on page 479
- Performing Threat Analysis using Casebooks, on page 481
- Improving User Experience of Cisco Web Security Appliance using Cisco Success Network, on page 484


## Integrating the Appliance with Cisco Threat Response

You can integrate your appliance with Cisco Threat Response, and perform the following actions in Cisco Threat Response:

- View the web tracking data from multiple appliances in your organization.
- Identify, investigate and remediate threats observed in web tracking.
- Resolve the identified threats rapidly and provide recommended actions to take against the identified threats.
- Document the threats in the portal to save the investigation, and enable collaboration of information among other devices on the portal.

To integrate your appliance with Cisco Threat Response, you need to register your appliance with Cisco Threat Response.

You can access Cisco Threat Response using the following URLs:

- https://visibility.amp.cisco.com (North Americas)
- https://visibility.eu.amp.cisco.com (Europe)
- https://visibility.apjc.amp.cisco.com (APJC)

**Note** If you have enabled and registered for CTR on your appliances, then the appliances automatically start sending the Cisco Success Network (CSN) telemetry data to Cisco. See Improving User Experience of Cisco Web Security Appliance using Cisco Success Network.

### Before you begin

- Access the CLI and enable the **reportingconfig** > **CTROBSERVABLE** command. When you enable the CTR observable indexing using this command, you can index the URLs accessed by the users. It also provides granularity to search any URLs in the appliance tracking database.
- You require a Cisco Security user account to access Cisco Threat Response. If any user in your organization already has a Cisco Security account, contact your system administrator. If you do not have a Cisco Security user account, you can create one at the Cisco Threat Response login page. Make sure that you create a user account in Cisco Threat Response with admin access rights. To create a new user account, go to the Cisco Threat Response login page using the following URL - https://visibility.amp.cisco.com (North Americas) or https://visibility.eu.amp.cisco.com (Europe) and click **Create a Cisco Security account** in the login page. If you are unable to create a new user account, contact Cisco TAC for assistance.
- Make sure that you enable Cisco Threat Response integration on the Cisco Security Services Exchange (SSE) portal. For more information, see the Cisco Threat Response documentation at https://visibility.amp.cisco.com/help/module-wsa (North Americas) or https://visibility.eu.amp.cisco.com/help/module-wsa (Europe).
- Make sure that you open HTTPS (Outbound) 443 port on the firewall for the following FQDNs to register your appliance with Cisco Threat Response:
  - api-sse.cisco.com (applicable for Americas users only)
  - api.eu.sse.itd.cisco.com (applicable for European Union (EU) users only)
  - api.apj.sse.itd.cisco.com (applicable for APJC users only)
  - est.sco.cisco.com (applicable for Americas, EU, and APJC users)
- Ensure that your DNS server can resolve the hostname configured on the management (M1) interface.

### Procedure

**Step 1** Log in to your appliance.

**Step 2** Select **Networks > Cloud Service Settings**.

**Step 3** Click **Edit Settings**.

**Step 4** Check **Enable**.

**Step 5** Submit and commit your changes.

**Step 6** Navigate back to the Cloud Service Settings page after few minutes to register your appliance with the Cisco Threat Response.

**Step 7** Choose your preferred server from the **Threat Response Server** drop-down list.

**Step 8** Obtain a registration token from Cisco Threat Response to register your appliance with the Cisco Threat Response. For more information, see the Cisco Threat Response documentation at https://visibility.amp.cisco.com/help/module-wsa (North Americas) or https://visibility.eu.amp.cisco.com/help/module-wsa (Europe).

**Step 9** Enter the registration token obtained from Cisco Threat Response and click **Register**.

**Step 10** Add your appliance as an integration module to Cisco Threat Response. For more information, see the Cisco Threat Response documentation at https://visibility.amp.cisco.com/help/module-wsa (North Americas) or https://visibility.eu.amp.cisco.com/help/module-wsa (Europe).

### What to do next

After you add your appliance as an integration module in Cisco Threat Response, you can view the web tracking information from your appliance in Cisco Threat Response. For more information, see the Cisco Threat Response documentation at https://visibility.amp.cisco.com/help/module-wsa (North Americas) or https://visibility.eu.amp.cisco.com/help/module-wsa (Europe).

**Note** To deregister your appliance connection from Cisco Threat Response, click **Deregister** in the Cloud Services Settings page in your appliance.

# Performing Threat Analysis using Casebooks

The casebook and pivot menu are widgets available in Cisco Threat Response.

Casebook - It is used to record, organize, and share sets of observables of interest primarily during an investigation and threat analysis. You can use a casebook to get the current verdicts or dispositions on the observables. For more information, see the Cisco Threat Response documentation at https://visibility.amp.cisco.com/help/casebooks for North Americas or https://visibility.eu.amp.cisco.com/help/casebooks for Europe regions.

Pivot Menu - It is used to perform threat response enabled tasks on observables directly from the Web Security appliance interface. These tasks can be performed through Cisco Threat Response or any of the user configured modules (for example, AMP for Endpoints, Cisco Umbrella, Cisco Talos Intelligence, and so on). For more information, see the Cisco Threat Response documentation at https://visibility.amp.cisco.com/help/pivot-menus for North Americas or https://visibility.eu.amp.cisco.com/help/pivot-menus for Europe regions.

The Web Security appliance now includes the casebook and pivot menu widgets. You can perform the following actions in your appliance using the casebook and pivot menu widgets:

- Add an observable to a casebook to investigate for threat analysis.
- Pivot an observable to a new case, an existing case, or other devices registered in Cisco Threat Response (for example, AMP for Endpoints, Cisco Umbrella, Cisco Talos Intelligence, and so on) to investigate for threat analysis.

The following is a list of observables that have the Threat Response pivot menus in the Web Security appliance user interface:

- IP addresses
- Domains
- URLs
- File Hashes (SHA-256 only)

**Note**

- The pivot menu widget is positioned next to the observables in the web reporting pages of your appliance.
- The casebook widget is positioned at the bottom-right corner of the web reporting pages of your appliance.

### Releted Topics

- Obtaining Client ID and Client Password Credentials, on page 482
- Adding Observable to Casebook for Threat Analysis, on page 483

# Obtaining Client ID and Client Password Credentials

You need the client ID and client password to access the casebook and pivot menu widgets on your appliance.

### Before you begin

Make sure that you meet all the prerequisites mentioned in the 'Before you begin' section of Integrating the Appliance with Cisco Threat Response, on page 479

### Procedure

**Step 1** Log in to the new web interface of your appliance.

**Step 2** Add a new API Client.

a) Click the **Threat Response API Clients** link.

When you click on the Threat Response API Clients link, it redirects you to the Cisco Threat Response login page.

b) Log in to Cisco Threat Response.

c) In Threat Response, click **Settings** and choose **API Clients** to go to the API Clients page.

d) Click **Add API Credentials**.

e) Enter the name of your appliance (for example, 'Web_Security_Appliance') as the client name.

f) Select the following scopes to provide full access to the casebook and pivot menu widgets:

- Casebook
- Enrich
- Private Intelligence
- Response
- Inspect

**Note**

- If you want to access the casebook widget only, select the following scopes - casebook, private intelligence, and inspect.
- If you want to access the pivot menu widget only, select the following scopes - enrich and response.

g) Click **Add New Client**.
h) Copy the client ID and client password to the clipboard.

**Note**
Make sure that you note the client ID and client password before you close the 'Add New Client' dialog box.

i) Click **Close**.

**Note**
If you want to add a new API client, you do not need to delete the existing API client.

**Step 3** Click the **Casebook** button.

**Step 4** Enter the client ID and client password obtained in Step 2 in the 'Login to use Casebook/Pivot Menu' dialog box in your appliance.

**Step 5** Select the required Cisco Threat Response server in the 'Login to use Casebook/Pivot Menu' dialog box.

**Step 6** Click **Authenticate**.

**Note**

If you want to edit the client ID, client password, and Cisco Threat Response server, right-click on the Casebook button and add the details.

### What to do next

Add an observable to a casebook to investigate for threat analysis. See Adding Observable to Casebook for Threat Analysis, on page 483

# Adding Observable to Casebook for Threat Analysis

### Before you begin

Make sure that you obtain the client ID and client password to access the casebook and pivot menu widgets on your appliance. For more information, see Obtaining Client ID and Client Password Credentials, on page 482.

### Procedure

**Step 1** Log in to the new web interface of your appliance.

**Step 2** Navigate to the Web Reporting page, click on the pivot menu button next to the required observable (for example, schemas.micrsoft.com) and click **Add to New Case** or **Add to Current Case**.

**Note**

- Use the drag and drop button next to the observable to drag and drop the observable into an existing case.

- Use the pivot menu button to take threat response enabled actions on observables using Cisco Threat Response or your other configured Cisco Threat Response modules (for example, blocking a domain using Umbrella, or blocking a file hash using AMP, or investigating an IP using all modules simultaneously).

**Step 3** Click the **Casebook** button to check whether the observable is added to a new or an existing case.

**Step 4** **(Optional)** Click button to add a title, description, or notes to the casebook.

**Step 5** Click **Investigate this Case** to investigate the observable for threat analysis. For more information, see the Cisco Threat Response documentation at https://visibility.amp.cisco.com/help/introduction (North Americas) or https://visibility.eu.amp.cisco.com/help/introduction (Europe).

# Improving User Experience of Cisco Web Security Appliance using Cisco Success Network

### Overview

You can use the Cisco Success Network (CSN) feature to send your appliance and feature usage details to Cisco. These details are used by Cisco to identify the device information, list of free and licensed features and their activation statuses.

The ability to send your appliance and feature usage details to Cisco helps an organization to:

- Improve the effectiveness of the product in user networks by performing analytics on collected telemetry data and suggesting users with recommendations using a digital campaign.
- Improve user experience with Cisco Web Security Appliace.

The following table shows a sample data of appliance and feature usage details sent to Cisco:

### Appliance Details

- Appliance model such as x90, x95, 100v, 300v, 600v.
- Appliance serial number and software version.
- Appliance installation date.
- Unique device identifier

### Feature Details

- Name of the feature.
- List of the features that are enabled.
- Staus of the feature (in compliance or not).
- Expiry date
- Feature Id

### Sample Data

**Note** For validating the telemetry data sent to Cisco, log subscription levels of *csid_logs* and *sse_connectord_log* should be in trace mode.

You can view the details in the *sse_connectord_log.current* in trace mode.


```
Thu May XX 10:48:30 2020 Trace: {
    "version": "0.X",
    "payload": {
        "recordVersion": "X.0",
        "recordedAt": 1589453310965,
        "deviceInfo": {
            "slVAN": "WSA",
            "installDate": 1589269184000,
            "version": "12.5.0-XXX",
            "userAccountID": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
            "model": "S600x",
            "udi": "XXXXXXXXXXXXXXXXXXXX-XXXXXXXXXXX"
        },
        "recordType": "CST_WSA",
        "features": {
            "free": [
                {
                    "enabled": "Y",
                    "featureName": "Smart Software Licensing"
                },
                {
                    "enabled": "N",
                    "featureName": "Identity Services Engine"
                },
                {
                    "enabled": "Y",
                    "featureName": "Cloud Services"
                },
                {
                    "enabled": "N",
                    "featureName": "Proxy Auto-Configuration File Hosting"
                },
                {
                    "enabled": "N",
                    "featureName": "Local Reporting Service"
                },
                {
                    "enabled": "Y",
                    "featureName": "Centralized Reporting Service"
                }
            ],
            "licensed": [
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Cisco Web Usage Controls",
                    "featureID":
"regid.2018-05.com.cisco.WSA-WUC,1.0_6e3a0734-ef40-4c60-bbcd-66ea1796231d",
                    "expiry": 1591803862000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Anti-Virus Webroot",
                    "featureID":
"regid.2018-05.com.cisco.WSA-AMW,1.0_794905fe-57e0-44df-8056-c1fc54f968d2",
```

```
                    "expiry": 1591803867000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance L4 Traffic Monitor",
                    "featureID":
"regid.2018-05.com.cisco.WSA_SB,1.0_c4b92628-15a4-4b73-94ad-9db1383054ce",
                    "expiry": 1591803872000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "N",
                    "featureName": "Web Security Appliance Cisco AnyConnect SM for
AnyConnect",
                    "featureID":
"regid.2018-05.com.cisco.WSA_MUS,1.0_d3f3389a-cdc4-48e3-bc84-8b590ea2d908",
                    "expiry": 1591803877000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Advanced Malware protection
Reputation",
                    "featureID":
"regid.2018-05.com.cisco.WSA_AMPREPU,1.0_a51bae61-c688-475a-aa19-51f86b52671e",
                    "expiry": 1591803893000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Anti-Virus Sophos",
                    "featureID":
"regid.2018-05.com.cisco.WSA-AMS,1.0_fda29c84-e1e7-4bb5-a220-f872e67bc44d",
                    "expiry": 1591803908000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Web Reputation Filters",
                    "featureID":
"regid.2018-05.com.cisco.WSA-WREP,1.0_37bb916e-65e2-4a55-ab3e-262d290c020a",
                    "expiry": 1591803857000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Advanced Malware Protection",
                    "featureID":
"regid.2018-05.com.cisco.WSA-AMP,1.0_34331e7c-0be5-4898-8563-a69c0a5fefba",
                    "expiry": 1591803882000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Anti-Virus McAfee",
                    "featureID":
"regid.2018-05.com.cisco.WSA-AMM,1.0_b8354876-14f5-4285-8dea-ca6a2bfb74c4",
                    "expiry": 1591803898000
                },
                {
                    "status": "IN_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Web Proxy and DVS Engine",
```

```
                    "featureID":
"regid.2018-05.com.cisco.WSA_WP,1.0_996c8b90-5305-43de-bdb8-bf48aa9d0457",
                    "expiry": 1591803903000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "N",
                    "featureName": "Web Security Appliance HTTPs Decryption",
                    "featureID":
"regid.2018-05.com.cisco.WSA_WD,1.0_563c38e7-7633-4cdc-a79f-3871d1284b57",
                    "expiry": 1591803887000
                }
            ]
        }
    },
    "metadata": {
        "topic": "wsa.telemetry",
        "contentType": "application/json"
    }
}
```


### Related Topics

- Enabling and Registering Cisco Success Network on the appliance, on page 487.
- Disabling Cisco Success Network, on page 488.

# Enabling and Registering Cisco Success Network on the appliance

### Before you begin

Make sure that you register your appliance with Cisco Threat Response. See Integrating the Appliance with Cisco Threat Response, on page 479

### Procedure

**Step 1** Go to **Network** > **Cloud Service Settings**.

**Step 2** In the **Settings** section, click **Edit Settings** and check the **Enable** checkbox next to **Threat Response**.

**Step 3** In the **Registration** section, perform the following steps:

a) Choose the appropriate threat response server from the drop-down list.

- AMERICAS (api-sse.cisco.com)
- EUROPE(api.eu.sse.itd.cisco.com)
- APJC(api.apj.sse.itd.cisco.com)

a) Enter the registration token generated through the Security Service Exchange (SSE) portal.

You must access the SSE portal and generate a token for registration.

b) Click **Register**.

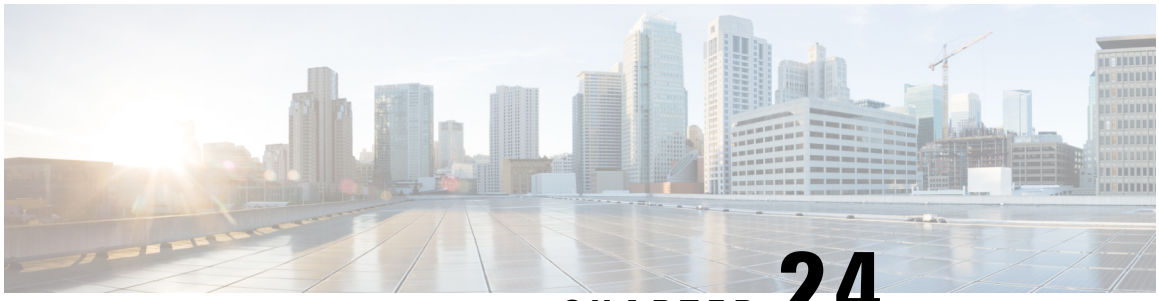
**Step 4** Submit and commit your changes.

To degister the appliance from Cisco Threat Response portal, click **Deregister**.

# Disabling Cisco Success Network

### Procedure

**Step 1** Go to **System Administration** > **Cisco Success Network**.
**Step 2** Click **Edit Settings** under Cisco Network Success.
**Step 3** Uncheck the **Enable** checkbox next to **Cisco Success Network**.
**Step 4** Submit and commit your changes.



CHAPTER 24

# Perform System Administration Tasks

This topic contains the following sections:


- Overview of System Administration, on page 489
- Saving, Loading, and Resetting the Appliance Configuration, on page 490
- Cisco Web Security Appliance  Licensing, on page 493
- Virtual Appliance License, on page 507
- Enabling Remote Power Cycling , on page 508
- Administering User Accounts, on page 509
- Defining User Preferences, on page 513
- Configuring Administrator Settings, on page 514
- User Network Access, on page 516
- Resetting the Administrator Passphrase, on page 517
- Configuring the Return Address for Generated Messages, on page 518
- Managing Alerts, on page 518
- FIPS Compliance, on page 529
- System Date and Time Management, on page 531
- SSL Configuration , on page 532
- Certificate Management, on page 533
- AsyncOS for Web Upgrades and Updates, on page 538
- Reverting to a Previous Version of AsyncOS for Web, on page 546
- Monitoring System Health and Status Using SNMP, on page 548
- Web Traffic Tap, on page 552


## 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, Loading, and Resetting 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, on page 490
- Saving the Appliance Configuration File, on page 490
- Loading the Appliance Configuration File, on page 491
- Resetting the Appliance Configuration to Factory Defaults , on page 492


## Viewing and Printing the Appliance Configuration

### Procedure

**Step 1** Choose **System Administration > Configuration Summary.**

**Step 2** View or print the Configuration Summary page as required.

## Saving the Appliance Configuration File

### Procedure

**Step 1** Choose **System Administration > Configuration File**.

**Step 2** Complete the Configuration File options.

| Option | Description |
|---|---|
| Specify a file-handling option | Choose how the generated configuration file is handled:<br>• Download file to local computer to view or save.<br>• **Save file to this appliance** (wsa_example.com).<br>• **Email file to:** – provide one or more email addresses. |
| Specify a passphrase-handling option | • **Mask passphrases in the Configuration Files**<br>– The original passphrases are replaced with "*****" in the exported or saved file. Please note that configuration files with masked passphrases cannot be loaded directly back into AsyncOS for Web.<br>• **Encrypt passphrases in the Configuration Files** – If FIPS mode is enabled, this option is available. See Enabling or Disabling FIPS Mode , on page 530 for information about enabling FIPS mode. |

| Option | Description |
|---|---|
| Select a file-naming option | Choose how the configuration file is named:<br>• **Use system-generated file name**<br>• **Use user-defined file name** |

**Step 3** Click **Submit**.

# Loading the Appliance Configuration File

**Caution** Loading configuration will permanently remove all of your current configuration settings. It is strongly recommended that you save your configuration before performing these actions.

We do not recommend loading configurations from a previous release into the latest version. You can retain the configuration settings by upgrading the paths.

Configuration files loaded with manual changes may result in performance and functional issues.

**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.

**Note** If you encounter a certificate validation error when loading the configuration file, upload the rootCA of the certificate to the trusted root directory of the Web Security Appliance and then load the configuration file again. To know how to upload the rootCA, see Certificate Management, on page 533.

## Procedure

**Step 1** Choose **System Administration > Configuration File**.

**Step 2** Choose Load Configuration options and a file to load. Note:

**Note**

- Files with masked passphrases 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**.

# Resetting the Appliance Configuration to Factory Defaults

You can choose whether or not to retain existing network settings when you reset the appliance configuration.

This action does not require a commit.

### Before you begin

Save your configuration to a location off the appliance.

### Procedure

**Step 1** Choose **System Administration > Configuration File**.

**Step 2** Scroll down to view the **Reset Configuration** section.

**Step 3** Read the information on the page and select options.

**Step 4** Click **Reset**.

# Saving Configuration File Backup

The configuration file backup feature records the appliance configuration on every commit and sends the previous configuration file before the current one to a remotely located backup server through FTP or SCP.

### Procedure

**Step 1** Choose **System Administration > Configuration File**

**Step 2** Select the **Enable Config Backup** check box.

**Step 3** Choose **Yes** to include the passphrase in the configuration file. Alternatively, choose **No** to exclude the passphrase in the configuration file.

**Step 4** Choose the retrieval method. The available options are:

- FTP on Remote Server - Enter the FTP hostname, directory, username, and passphrase.
- SCP on Remote Server- Enter the SCP hostname, port number, directory, and username.
- Host Key Checking- The SSH automatically maintains and checks a database of identifications for all hosts with which it has been used. Host keys are stored in the user's home directory in the directory */.ssh/known_hosts*.

  If you select **SCP on Remote Server** and then select **Enable Host Key Checking**, you will have the following options:

  - Automatic- The host key will be set automatically by Secure Web Appliance.

- Manual- User can enter the host key manually.

Upon submitting the changes, Secure Web Appliance provides SSH key(s) to be added to authorized keys file on remote host, so that configuration files can be uploaded from Secure Web Appliance to the remote host. As a result, SSH maintains and checks a database containing identification information for all hosts it has ever connected to. Host keys are stored in the user's home directory in the directory */.ssh/known_hosts*.

**Step 5** Click **Submit**.

You can also enable the configuration file backup feature by using the CLI command `configbackup`

# Cisco Web Security Appliance  Licensing


- Working with Feature Keys, on page 493
- Smart Software Licensing, on page 494


## 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).


- Displaying and Updating Feature Keys, on page 493
- Changing Feature Key Update Settings , on page 494


### Displaying and Updating Feature Keys

#### Procedure

**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.

### Procedure

**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.<br>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.

# Smart Software Licensing


- Overview, on page 494
- Enabling Smart Software Licensing , on page 496
- Registering the Appliance with Cisco Smart Software Manager , on page 497
- Requesting for Licenses, on page 499
- Deregistering the Appliance from Smart Cisco Software Manager, on page 500
- Reregistering the Appliance with Smart Cisco Software Manager, on page 501
- Changing Transport Settings, on page 501
- Renewing Authorization and Certificate, on page 501
- Updating Smart Agent, on page 502
- Alerts, on page 502
- Command Line Interface, on page 503


## Overview

Smart Software Licensing enables you to manage and monitor Cisco Web Security Appliance licenses seamlessly. To activate Smart Software licensing, you must register your appliance with Cisco Smart Software

Manager (CSSM) which is the centralized database that maintains the licensing details about all the Cisco products that you purchase and use. With Smart Licensing, you can register with a single token rather than registering them individually on the website using Product Authorization Keys (PAKs).

Once you register the appliance, you can track your appliance licenses and monitor license usage through the CSSM portal. The Smart Agent installed on the appliance connects the appliance with CSSM and passes the license usage information to the CSSM to track the consumption.

See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html to know about Cisco Smart Software Manager.

**Note** AsyncOS version 15.0 is the last release to support the Classic license. The next releases will only support Smart Licenses.

### Before you begin

- Make sure that your appliance has internet connectivity.
- Contact Cisco sales team to create a smart account in Cisco Smart Software Manager portal (https://software.cisco.com/#module/SmartLicensing) or install a Cisco Smart Software Manager Satellite on your network.

  See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html to know more about Cisco Smart Software Manager user account creation or installing a Smart Software Manager On-Prem.

  For users who do not want to directly send the license usage information to the internet, the Smart Software Manager Satellite can be installed on the premises, and it provides a subset of CSSM functionality. Once you download and deploy the satellite application, you can manage licenses locally and securely without sending data to CSSM using the internet. The CSSM Satellite periodically transmits the information to the cloud.

**Note** If you want to use Smart Software Manager Satellite, use Smart Software Manager Satellite Enhanced Edition 6.1.0.

- The existing users of classic licenses (traditional) should migrate their classic licenses to smart licenses.

  See https://video.cisco.com/detail/video/6330894176112?autoStart=true&q=convert-classic-licenses-to-smart-licenses.
- The system clock of the appliance must be in sync with that of the CSSM. Any deviation in the system clock of the appliance with that of the CSSM, will result in failure of smart licensing operations.

**Note** If you have internet connectivity and want to connect to the CSSM through a proxy, you must use the same proxy that is configured for the appliance using **System Administration-> Upgrade and Update Settings**

**Note** For virtual users, every time you receive a new PAK file (new or renewal), generate the license file and load the file on the appliance. After loading the file, you must convert the PAK to Smart Licensing. In Smart Licensing mode, the feature keys section in the license file will be ignored while loading the file and only the certificate information will be used.

**Note** The appliance will move from the Smart Licensing mode to Classic Licensing mode when you revert the appliance to a previous veriosn of AsyncOS. You must enable Smart Licensing manually and request for required licences.

You must perform the following procedures to activate Smart Software Licensing for your appliance:

| | Do This | More Informaton |
|---|---|---|
| Step 1 | Enable Smart Software Licensing | Enabling Smart Software Licensing , on page 496 |
| Step 2 | Register the appliance with Cisco Smart Software Manager | Registering the Appliance with Cisco Smart Software Manager , on page 497 |
| Step 3 | Request for licenses (feature keys) | Requesting for Licenses, on page 499 |

## Enabling Smart Software Licensing

### Procedure

**Step 1** Choose **System Administration > Smart Software Licensing**.

**Step 2** Click **Enable Smart Software Licensing**.

To know about Smart Software Licensing, click on the **Learn More about Smart Software Licensing** link.

**Step 3** Click **OK** after reading the information about Smart Software Licensing.

**Step 4** Commit your changes.

### What to do next

After you enable Smart Software Licensing, all the features in the Classic Licensing mode will be automatically available in the Smart Licensing mode. If you are an existing user in Classic Licensing mode, you have 90-days evaluation period to use the Smart Software Licensing feature without registering your appliance with the CSSM.

You will get notifications on regular intervals (90th, 60th, 30th, 15th, 5th, and last day) prior to the expiry and also upon expiry of the evaluation period. You can register your appliance with the CSSM during or after the evaluation period.



**Note**

- New Virtual Appliance users with no active licenses in Classic Licensing mode will not have the evaluation period even if they enable the Smart Software Licensing feature. Only the existing Virtual Appliance users with active licenses in Classic Licensing mode will have evaluation period. If new Virtual Appliance users want to evaluate the smart licensing feature, contact Cisco Sales team to add the evaluation license to the smart account. The evaluation licenses are used for evaluation purpose after registration.
- After you enable the Smart Licensing feature on your appliance, you will not be able to roll back from Smart Licensing to Classic Licensing mode.
- The following features are restarted when you enable the Smart Licensing feature:
  - Web Security Appliance  Web Reputation Filters
  - Web Security Appliance  Anti-Virus Sophos
  - Web Security Appliance  Anti-Virus Webroot
  - Web Security Appliance  Web Proxy and DVS Engine
- In AsyncOS version 15.0, Smart Licensing can be enabled for new Secure Web Appliance virtual deployments. Even though Classic licensing is not mandatory. For more information, refer to the pre-requisites available under the Overview of Smart Licencing section.

## Registering the Appliance with Cisco Smart Software Manager

You must enable the Smart Software Licensing feature under System Administration menu in order to register your appliance with the Cisco Smart Software Manager.



**Note** You cannot register multiple appliances in a single instance. You should register appliances one by one.

### Procedure

**Step 1** Choose **System Administration** > **Smart Software Licensing**.

**Step 2** Select the **Smart License Registration** option.

**Step 3** Click **Confirm**.

**Step 4** Click **Edit**, if you want to change the Transport Settings. The available options are:

- **Direct**: Connects the appliance directly to the Cisco Smart Software Manager through HTTPs. This option is selected by default.
- **Transport Gateway**: Connects the appliance to the Cisco Smart Software Manager through a Transport Gateway or Smart Software Manager Satellite. When you choose this option, you must enter the URL of the Transport Gateway

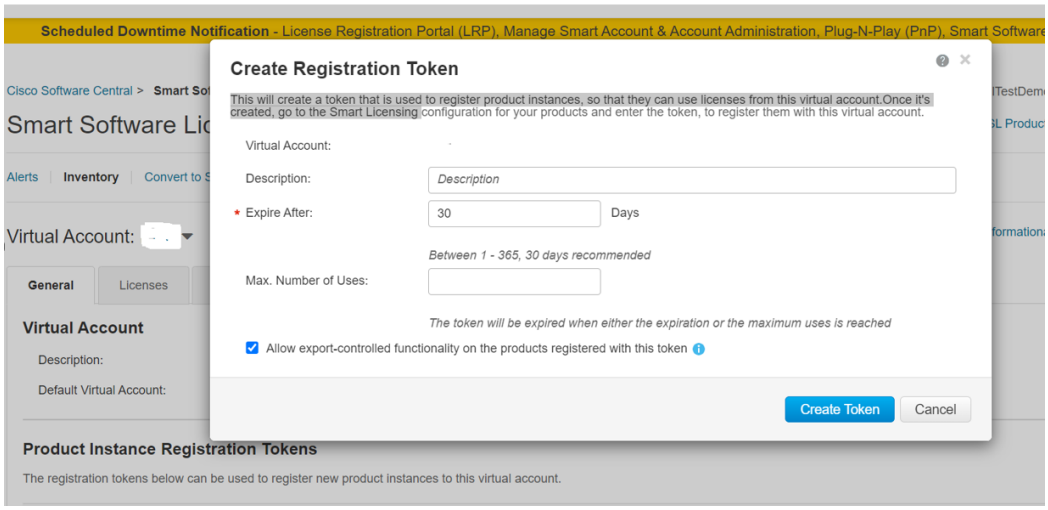
or the Smart Software Manager Satellite and click OK. This option supports HTTP and HTTPS. In FIPS mode, Transport Gateway supports only HTTPS.

See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html to know about Transport Gateway.

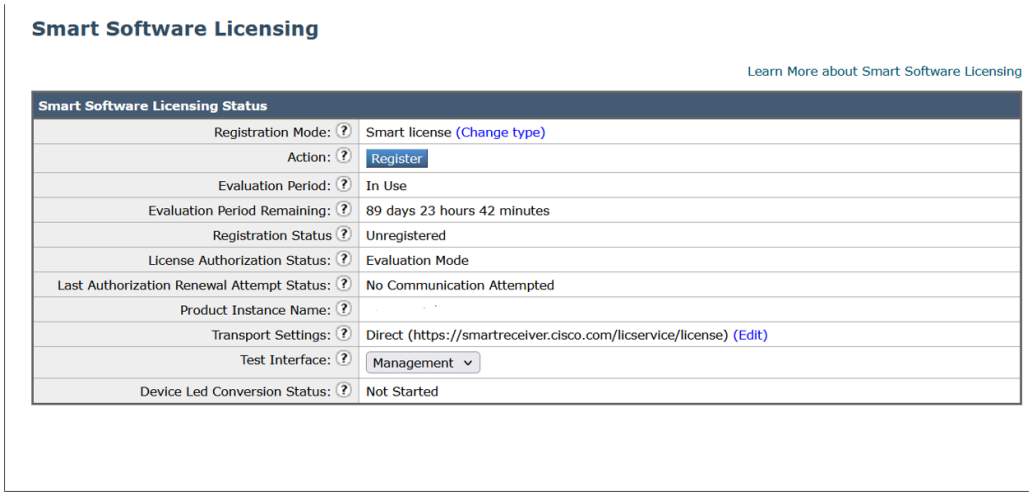
**Step 5** (Optional) **Test Interface**: Choose Management or Data interface while registering the appliance for the smart licensing feature. This is applicable only when you enable split routing and register for smart licensing.

**Note**
If split routing is not enabled, only Management interface option is available in the **Test Interface** drop-down list.

**Step 6** Access the Cisco Smart Software Manager portal (https://software.cisco.com/#module/SmartLicensing) using your login credentials. Navigate to the Virtual Account page of the portal and access the General tab to generate a new token. Copy the Product Instance Registration Token for your appliance. See https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_ Deployment_Guide.html to know about Product Instance Registration Token creation.

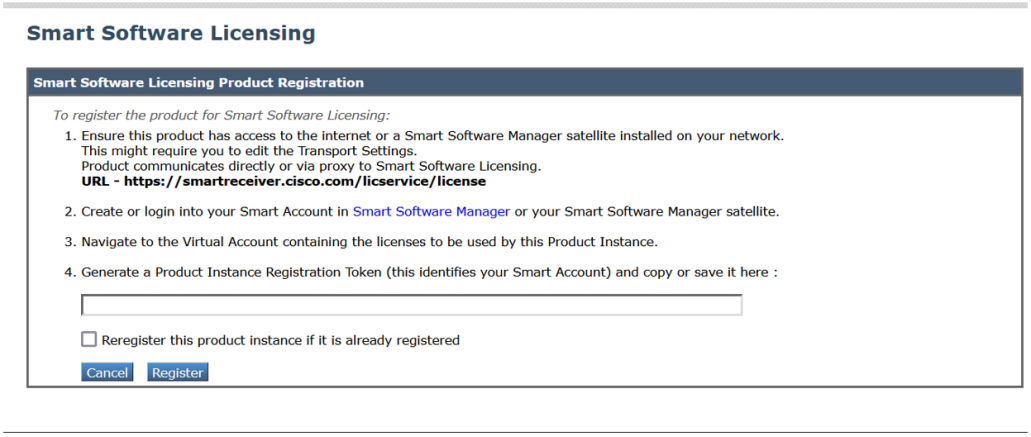



**Step 7** Switch back to your appliance and click **Register**.



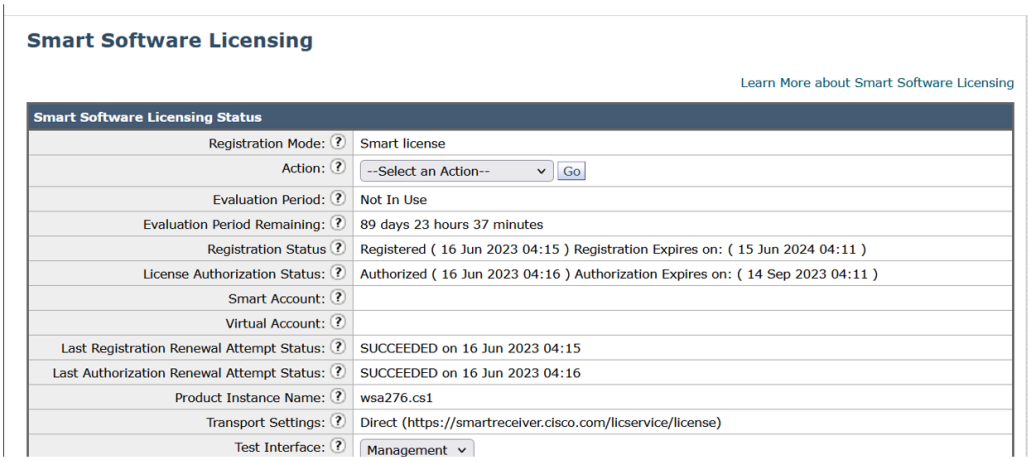
**Step 8** Paste the **Product Instance Registration Token** in the textbox.

On the Smart Software Licensing page, you can select the **Reregister this product instance if it is already registered** check box to reregister your appliance.




### What to do next

The product registration process takes a few minutes and you can view the registration status on the Smart Software Licensing page.




## Requesting for Licenses

Once you complete the registration process successfully, you must request for licenses for the appliance's features as required.

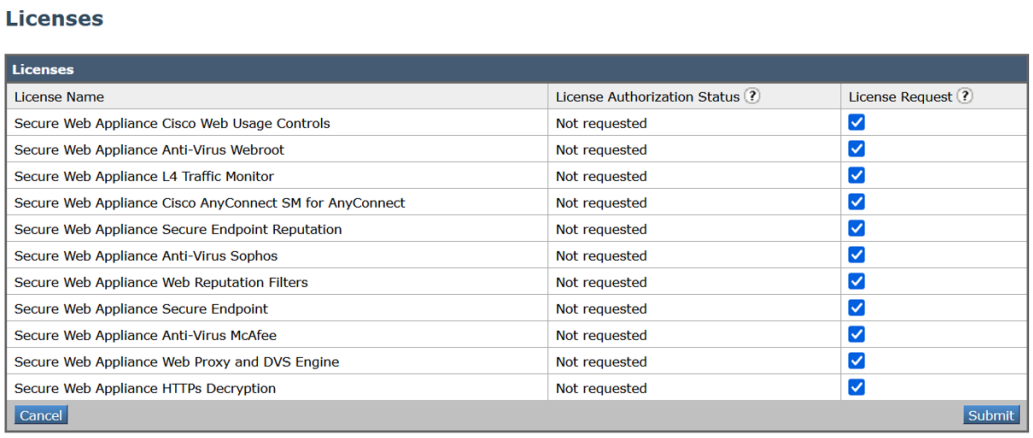
### Procedure

**Step 1** Choose **System Administration > Licenses**.

**Step 2** Click **Edit Settings**.

**Step 3** Check the checkboxes under the License Request/Release column corresponding to the licenses you want to request for.

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




### What to do next

When the licenses are overused or expired, they will go into out of compliance (OOC) mode and 30-days grace period is provided to each license. You will get notifications on regular intervals (30th, 15th, 5th, and last day) prior to the expiry and also upon the expiry of the OOC grace period.

After the expiry of the OOC grace period, you cannot use the licenses and the features will be unavailable. To access the features again, you must update the licenses on the CSSM portal and renew the authorization.

### Releasing Licenses

#### Procedure

**Step 1** Choose **System Administration > Licenses**.

**Step 2** Click **Edit Settings**.

**Step 3** Uncheck the checkboxes under the License Request column corresponding to the licenses you want to release.

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

## Deregistering the Appliance from Smart Cisco Software Manager

#### Procedure

**Step 1** Choose **System Administration > Smart Software Licensing**.

**Step 2** From the **Action** drop-down list, choose **Deregister** and click **Go**.

**Step 3** Click **Submit**.

## Reregistering the Appliance with Smart Cisco Software Manager

### Procedure

**Step 1** Choose **System Administration > Smart Software Licensing**.

**Step 2** From the **Action** drop-down list, choose **Reregister** and click **Go**.

#### What to do next

See Registering the Appliance with Cisco Smart Software Manager , on page 497 to know about registration process.

You can reregister the appliance after you reset the appliance configurations during unavoidable scenarios.

## Changing Transport Settings

You can change the transport settings only before registering the appliance with CSSM.

**Note** You can change the transport settings only when the smart licensing feature is enabled.If you have already registered your appliance, you must deregister the appliance to change the transport settings. After changing the transport settings, you must register the appliance again.

See Registering the Appliance with Cisco Smart Software Manager , on page 497 to know how to change the transport settings.

## Renewing Authorization and Certificate

After you register your appliance with the Smart Cisco Software Manager, you can renew the certificate.

**Note** You can renew authorization only after the successful registration of the appliance.

### Procedure

**Step 1** Choose **System Administration > Smart Software Licensing**.

**Step 2** From the **Action** drop-down list, choose the appropriate option:

- **Renew Authorization Now**
- **Renew Certificates Now**

**Step 3** Click **Go**.

### What to do next

## Updating Smart Agent

To update the Smart Agent version installed on your appliance, perform the following steps:

### Procedure

**Step 1** Choose **System Administration > Smart Software Licensing**.

**Step 2** In the **Smart Agent Update Status** section, click **Update Now** and follow the process.

**Note**
If you try to save any configuration changes using the CLI command `saveconfig` or through the web interface using **System Administration > Configuration Summary**, then Smart Licensing related configuration will not be saved.

## Alerts

You will receive notifications on the following scenarios:

- Smart Software Licensing successfully enabled
- Smart Software Licensing enabling failed
- Beginning of the evaluation period
- Expiry of evaluation period (on regular intervals during evaluation period and upon expiry)
- Successfully registered
- Registration failed
- Successfully authorized
- Authorization failed
- Successfully deregistered
- Deregistration failed
- Successfully renewed Id certificate
- Renewal of Id certificate failed
- Expiry of authorization
- Expiry of Id certificate
- Expiry of out of compliance grace period (on regular intervals during out of compliance grace period and upon expiry).

- First instance of the expiry of a feature

## Command Line Interface


- license_smart, on page 503
- show_license, on page 506


### license_smart


- Description, on page 503
- Usage, on page 503
- Example: Configuring Port for Smart Agent Service, on page 503
- Example: Enabling Smart Licensing, on page 503
- Example: Registering the Appliance with the Smart Software Manager , on page 504
- Example: Status of Smart Licensing , on page 504
- Example: Status Summary of Smart Licensing , on page 505
- Example: Setting the Smart Transport URL, on page 505
- Example: Requesting Licenses, on page 505
- Example: Releasing Licenses, on page 506


#### *Description*

Configure smart software licensing feature.

#### *Usage*

**Commit**: This command requires a 'commit'.

**Batch Command**: This command supports a batch format. For details, see the inline help by typing the command: `help license_smart`.

#### *Example: Configuring Port for Smart Agent Service*

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
- SETAGENTPORT - Set port to run Smart Agent service.
[]> setagentport

Enter the port to run smart agent service.
[65501]>
```

#### *Example: Enabling Smart Licensing*

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
 []> enable
After enabling Smart Licensing on your appliance, follow below steps to activate
```

```
the feature keys (licenses):

a) Register the product with Smart Software Manager using license_smart > register command
 in the CLI.
b) Activate the feature keys using license_smart > requestsmart_license command in the CLI.

Note: If you are using a virtual appliance, and have not enabled any of the
features in the classic licensing mode; you will not be able to activate the
licenses, after you switch to the smart licensing mode. You need to first register
your appliance, and then you can activate the licenses (features) in the smart licensing
mode.
Commit your changes to enable the Smart Licensing mode on your appliance.
All the features enabled in the Classic Licensing mode will be available in the Evaluation
 period.
Type "Y" if you want to continue, or type "N" if you want to use the classic licensing mode
 [Y/N] []> y

> commit

Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
```

### *Example: Registering the Appliance with the Smart Software Manager*

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> register
Reregister this product instance if it is already registered [N]> n

Enter token to register the product:
[]>
ODRlOTM5MjItOTQzOS00YjY0LWExZTUtZTdmMmY3OGNlNDZmLTE1MzM3Mzgw%0AMDEzNTR8WlpCQ1lMbGVMQWRx
OXhuenN4OWZDdktFckJLQzF5V3VIbzkyTFgx%0AQWcvaz0%3D%0A
Product Registration is in progress. Use license_smart > status command to check status of
 registration.
```

### *Example: Status of Smart Licensing*

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered
```

```
License Authorization Status: Evaluation Mode

Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

### *Example: Status Summary of Smart Licensing*

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> summary

FeatureName                                  LicenseAuthorizationStatus
Web Security Appliance Cisco                 Eval
Web Usage Controls
Web Security Appliance Anti-Virus Webroot    Eval
Web Security Appliance Anti-Virus Sophos     Eval
```

### *Example: Setting the Smart Transport URL*

```
example.com> license_smart

Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> url

1. DIRECT - Product communicates directly with the cisco license servers
2. TRANSPORT_GATEWAY - Product communicates via transport gateway or smart software manager
 satellite.

Choose from the following menu options:
[1]> 1
Note: The appliance uses the Direct URL
(https://smartreceiver.cisco.com/licservice/license) to communicate with Cisco
Smart Software Manager (CSSM) via the proxy server configured using the updateconfig command.
Transport settings will be updated after commit.
```

### *Example: Requesting Licenses*



**Note** Users of virtual appliance must register their appliance to request for or release the licenses.

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
```

```
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> requestsmart_license

Feature Name                                    License Authorization Status
1. Web Security Appliance Anti-Virus Sophos      Not Requested
2. Web Security Appliance                        Not requested
   L4 Traffic Monitor

Enter the appropriate license number(s) for activation.
Separate multiple license with comma or enter range:
[]> 1
Activation is in progress for following features:
Web Security Appliance Anti-Virus Sophos
Use license_smart > summary command to check status of licenses.
```

*Example: Releasing Licenses*

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> releasesmart_license

Feature Name                                  License Authorization Status
1. Web Security Appliance Cisco               Eval
   Web Usage Controls
2. Web Security Appliance                     Eval
   Anti-Virus Webroot
3. Web Security Appliance                     Eval
   L4 Traffic Monitor
4. Web Security Appliance Cisco               Eval
   AnyConnect SM for AnyConnect
5. Web Security Appliance Advanced            Eval
   Malware Protection Reputation
6. Web Security Appliance                     Eval
   Anti-Virus Sophos
7. Web Security Appliance                     Eval
   Web Reputation Filters
8. Web Security Appliance Advanced            Eval
   Malware Protection
```

## show_license


- Description, on page 506
- Example: Status of Smart Licensing, on page 507
- Example: Status Summary of Smart Licensing, on page 507


*Description*

Show Smart Licensing status and summary of status.

*Example: Status of Smart Licensing*

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> status
Smart Licensing is: Enabled
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: example.com
Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

*Example: Status Summary of Smart Licensing*

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.

[]> summary

FeatureName                          LicenseAuthorizationStatus
Web Security Appliance Cisco         Eval
Web Usage Controls
Web Security Appliance               Eval
Anti-Virus Webroot
Web Security Appliance               Eval
Anti-Virus Sophos
```

# Virtual Appliance License

The Cisco Web Security Virtual appliance requires an additional license to run the virtual appliance on a host.

For more information about virtual appliance licensing, see the *Cisco Content Security Virtual Appliance Installation Guide* , available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

**Note** You cannot open a Technical Support tunnel before installing the virtual appliance license.

After the license expires, the appliance will continue to serve as a web proxy without security services for180 days. Security service updates do not occur during this period.

You can configure the appliance so you receive alerts about license expiration.

### Related Topics

- Managing Alerts, on page 518

# Installing a Virtual Appliance License

See the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html

# Enabling Remote Power Cycling

### Before you begin

- Cable the dedicated Remote Power Cycle (RPC) port directly to a secure network. For information, see the hardware guide for your appliance model. For the location of this document, see Documentation Set, on page 613.
- Ensure that the appliance is accessible remotely; for example, open any necessary ports through the firewall.
- This feature requires a unique IPv4 address for the dedicated Remote Power Cycle interface. This interface is configurable only via the procedure described in this section; it cannot be configured using the ipconfig command.
- In order to cycle appliance power, you will need a third-party tool that can manage devices that support the Intelligent Platform Management Interface (IPMI) version 2.0. Ensure that you are prepared to use such a tool.
- For more information about accessing the command-line interface, see Command Line Interface, on page 587

The ability to remotely reset the power for the appliance chassis is available on x80, x90, and x95 series hardware.

If you want to be able to remotely reset appliance power, you must enable and configure this functionality in advance, using the procedure described in this section.

### Procedure

**Step 1** Use SSH or the serial console port to access the command-line interface.

**Step 2** Sign in using an account with Administrator access.

**Step 3** Enter the following commands:

```
remotepower
setup
```

**Step 4** Follow the prompts to specify the following:

- The dedicated IP address for this feature, plus netmask and gateway.
- The username and passphrase required to execute the power-cycle command.

  These credentials are independent of other credentials used to access your appliance.

**Step 5** Enter `commit` to save your changes.

**Step 6** Test your configuration to be sure that you can remotely manage appliance power.

**Step 7** Ensure that the credentials that you entered will be available to you in the indefinite future. For example, store this information in a safe place and ensure that administrators who may need to perform this task have access to the required credentials.

### What to do next

### Related Topics

- Hardware Appliances: Remotely Resetting Appliance Power , on page 577

# Administering User Accounts

The following types of users can log into the appliance to manage it:

- **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 LDAP or 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, on page 509
- RADIUS User Authentication, on page 512
- Configuring External Authentication through an LDAP Server, on page 100

# 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 passphrase, but you cannot edit or delete this account.

**Note** If you have lost the admin user passphrase, contact your Cisco support provider. For more details, see Reset Your Administrator Password and Unlock the Administrator User Account.

# Adding Local User Accounts

### Before you begin

Define the passphrase requirements that all user accounts must follow. See Setting Passphrase Requirements for Administrative Users , on page 514.

### Procedure

**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 `upgradecheck` and `upgradeinstall` 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:<br>• `resetconfig`<br>• `upgradecheck`<br>• `upgradeinstall`<br>The operators group restricts the use of System Setup Wizard as well. |
| Read-Only Operator | User accounts with this role:<br>• Can view configuration information.<br>• Can make and submit changes to see how to configure a feature, but they cannot commit them.<br>• Cannot make any other changes to the appliance, such as clearing the cache or saving files.<br>• 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 or generate a passphrase.

**Step 7** Submit and commit your changes.

## Deleting User Accounts

### Procedure

**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

### Procedure

**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 Passphrases

To change the passphrase of the account currently logged in, select **Options** > **Change Passphrase** from the top right-hand side of the window.

For other accounts, edit the account and change the passphrase in the Local User Settings page.

### Related Topics

- Editing User Accounts, on page 511
- Setting Passphrase Requirements for Administrative Users , on page 514

## Configuring Restrictive User Account and Passphrase Settings

You can define user account and passphrase restrictions to enforce organizational passphrase policies. The user account and passphrase restrictions apply to local users defined on the Cisco appliance. You can configure the following settings:

- **User account locking.**You can define how many failed login attempts cause the user to be locked out of the account. You can set the number of user login attempts from 1 to 60. The default value is 5.
- **Passphrase lifetime rules.**You can define how long a passphrase can exist before the user is required to change the passphrase after logging in.

- **Passphrase rules.** You can define what kinds of passphrases users can choose, such as which characters are optional or mandatory.

You define user account and passphrase restrictions on the System Administration > Users page in the Local User Account & Passphrase Settings section.

# 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 groups of external users 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 passphrase, access to the appliance is denied.

## Enabling External Authentication Using RADIUS

### Procedure

**Step 1** On the **System Administration > Users** page, click **Enable External Authentication**.

**Step 2** Choose **RADIUS** as the Authentication Type.

**Step 3** Enter the host name, port number, and Shared Secret passphrase for the RADIUS server. Default port is `1812`.

**Step 4** Enter the number of seconds the appliance is 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 1 – 5** for each RADIUS server.

**Note**
You can add up to ten RADIUS servers.

**Step 7** In the **External Authentication Cache Timeout** field, enter the number of seconds AsyncOS stores the external authentication credentials before contacting the RADIUS server again to re-authenticate. Default is zero.

**Note**
If the RADIUS server uses one-time passphrases, for example passphrases 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—Select whether to map all externally authenticated users to the Administrator role or to different appliance-user role types.

| Setting | Description |
|---|---|
| Map externally authenticated users to multiple local roles. | Enter a group name as defined in the RADIUS CLASS attribute, and choose an appliance Role type. You can add more role mappings by clicking Add Row.<br><br>AsyncOS assigns RADIUS users to appliance roles based on the RADIUS CLASS attribute. CLASS attribute requirements:<br><br>• three-character minimum<br>• 253-character maximum<br>• no colons, commas, or newline characters<br>• one or more mapped CLASS attributes for each RADIUS user (With this setting, AsyncOS denies access to RADIUS users without a mapped CLASS attribute.)<br><br>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.<br><br>These are the appliance roles ordered from most restrictive to least restrictive:<br><br>• Administrator<br>• Operator<br>• Read-Only Operator<br>• Guest |
| Map all externally authenticated users to the Administrator role. | AsyncOS assigns all RADIUS users to the Administrator role. |

**Step 9** Submit and commit your changes.

### What to do next

### Related Topics

- External Authentication, on page 100
- Adding Local User Accounts, on page 510.

# 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.

**Procedure**

**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

## Setting Passphrase Requirements for Administrative Users

To set passphrase requirements for locally-defined administrative users of the appliance:

**Procedure**

**Step 1** Select **System Administration** > **Users**.

**Step 2** In the **Passphrase Settings** section, click **Edit Settings**.

**Step 3** Choose options:

| Option | Description |
|---|---|
| List of words to disallow in passphrases | Create a .txt file with each forbidden word on a separate line, then select the file to upload it. Subsequent uploads overwrite previous uploads. |

| Option | Description |
|---|---|
| Passphrase Strength | You can display a passphrase-strength indicator when an administrative user enters a new passphrase.<br>This setting does not enforce creation of strong passphrases, it merely shows how easy it is to guess the entered passphrase.<br>Select the roles for which you wish to display the indicator. Then, for each selected role, enter a number greater than zero. A larger number means that a passphrase that registers as strong is more difficult to achieve. This setting has no maximum value, but a very high number makes it effectively impossible to enter a passphrase that evaluates as "good."<br>Experiment to see what number best meets your requirements.<br>Passphrase strength is measured on a logarithmic scale. Evaluation is based on the U.S. National Institute of Standards and Technology rules of entropy as defined in NIST SP 800-63, Troubleshooting topic.<br>Generally, stronger passphrases:<br>• Are longer<br>• Include upper case, lower case, numeric, and special characters<br>• Do not include words in any dictionary in any language.<br>To enforce passphrases with these characteristics, use the other settings on this page. |

**Step 4** Submit and commit your changes.

# Additional Security Settings for Accessing the Appliance

You can use the CLI command `adminaccessconfig` to 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 log in. The custom log-in banner appears when an administrator accesses the appliance through any interface; for example, via the Web UI, CLI, or FTP.<br>You can load the custom text either by pasting it into the CLI prompt, or by copying it from a text 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` > `welcome` | This is a post-log-in banner, displayed after successful administrator log-in. This text is added to the appliance configuration by the same means as the log-in `adminaccessconfig` > `banner` text. |

| Command | Description |
|---|---|
| `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.<br>When restricting 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. This information also can be provided using the Web UI; see User Network Access, on page 516. |
| `adminaccessconfig > csrf` | Enable/disable Web UI cross-site request forgery protection, used to identify and protect against malicious or spoofed requests. For best security, it is recommended that CSRF protection be enabled. |
| `adminaccessconfig > hostheader` | Configure use of host header in HTTP requests.<br>By default, the Web UI responds with the host header sent by the Web client in an HTTP request. For increased security, you can configure the Web UI to respond with only the appliance-specific host name; that is, the appliance's configured name (for example, `wsa_04.local`). |
| `adminaccessconfig > timeout` | Provide an inactivity time-out interval; that is, the number of minutes users can be inactive before being logged out. This value can be between five and 1440 minutes (24 hours); the default value is 30 minutes. This information also can be provided using the Web UI; see User Network Access, on page 516. |
| `adminaccessconfig > how-tos` | Enable walkthroughs that assist you in accomplishing specific configuration tasks. |
| `adminaccessconfig > strictssl` | Configures the appliance so administrators log into the web interface on port 8443 using stronger SSL ciphers (greater than 56 bit encryption).<br>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. |
| `adminaccessconfig > loginhistory` | Configure the number of days for which the login history is retained. |
| `adminaccessconfig > maxsessions` | Configure the maximum number of concurrent login sessions (CLI and web interface). |

# User Network Access

You can specify how long a user can be logged into the appliance before AsyncOS logs the user out due to inactivity. You also can specify the type of user connections allowed.

The session timeout applies to all users, including administrators, logged into either the Web UI or the CLI. When AsyncOS logs a user out, the user is redirected to the appliance log-in page.

**Note** You also can use the CLI `adminaccessconfig` > `timeout` to set this time-out value.

### Procedure

**Step 1** Choose **System Administration** > **Network Access**.

**Step 2** Click **Edit Settings**.

**Step 3** In the **Session Inactivity Timeout** field, enter the number of minutes users can be inactive before being logged out.

You can define a time-out interval between five and 1440 minutes (24 hours); the default value is 30 minutes.

**Step 4** In the **User Access** section, you control users' system access: choose either **Allow Any Connection** or **Only Allow Specific Connections**.

If you choose **Only Allow Specific Connections**, define the specific connections as IP addresses, IP ranges, or CIDR ranges. Along with the client IP address, the appliance IP address is automatically added in the **User Access** section.

**Step 5** Submit and commit your changes.

# Resetting the Administrator Passphrase

### Before you begin

- If you do not know the passphrase for the admin account, contact your customer support provider to reset the passphrase.
- Understand that changes to the passphrase take effect immediately and do not require you to commit the change.

Any administrator-level user can change the passphrase for the "admin" user.

### Procedure

**Step 1** Select **Management Appliance** > **System Administration** > **Users**.

**Step 2** Click the **admin** link in the Users list.

**Step 3** Select **Change the passphrase**.

**Step 4** Generate or enter the new passphrase.

# Configuring the Return Address for Generated Messages

You can configure the return address for mail generated by AsyncOS for reports.

**Procedure**

**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 . 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
- AMP
- L4 Traffic Monitor
- External URL Categories
- Policy Expiration

## 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

### Procedure

**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

### Procedure

**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.

**Procedure**

**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:<br>**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.<br>**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 |

**Note**
From AsyncOS 12.0, Cisco AutoSupport option is removed from the alert settings. You can only enable or disable AutoSupport fuctionality using the **alertconfig** CLI.

**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.

## 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:<br>$error | Warning | **$error:** Text of the RAID error. |

## 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.<br>**$message:** Error message text. |
| System halt failed: $exit_status: $output', | Critical. | **$exit_status:** Exit code of the command.<br>**$output:** Output from the command. |
| System reboot failed: $exit_status: $output | Critical. | **$exit_status:** Exit code of the command.<br>**$output:** Output from the command. |
| Process $name listed $dependency as a dependency, but it does not exist. | Critical. | **$name:** Name of the process.<br>**$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.<br>**$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.<br>**$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:<br>Error: $error. | Warning. | **$error:** The error message associated with the exception. |

| Message | Alert Severity | Parameters |
|---|---|---|
| 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. |
| Appliance: $appliance, User: $username, Source IP: $ip, Event: Account locked due to X failed login attempts.<br>User $username is locked after X consecutive login failures. Last login attempt was from $ip. | Information. | **$appliance**: Identifier of the specific Web Security Appliance .<br>**$username**: Identifier of the specific user account.<br>**$ip**: - IP address from which the login attempt occurred. |
| Tech support: Service tunnel has been enabled, port $port | Information. | **$port:** Port number used for the service tunnel. |
| Tech support: Service tunnel has been disabled. | Information. | Not applicable. |
| • The host at $ip has been added to the blocked list because of an SSH DOS attack.<br>• The host at $ip has been permanently added to the ssh allowed list.<br>• The host at $ip has been removed from the blocked list. | Warning. | **$ip** - IP address from which a login attempt occurred.<br>**Description:**<br>IP addresses that try to connect to the appliance over SSH but do not provide valid credentials are added to the SSH blocked list if more than 10 failed attempts occur within two minutes.<br>When a user logs in successfully from the same IP address, that IP address is added to the allowed list.<br>Addresses on the allowed list are allowed access even if they are also on the blocked list.<br>Entries are automatically removed from the blocked list after about a day. |

**Note** System alerts include Feature Key Alerts, Logging Alerts, and Reporting Alerts. You will receive these alerts after configuring them as part of the system alerts.

## 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.<br>**$days:** The number of days that will pass before the feature key will expire. |

## 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.<br>**$ip:** IP address of the remote host.<br>**$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.<br>**$ip:** IP address of the remote host.<br>**$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.<br>**$ip:** IP address of the remote host.<br>**$port:** Port number on the remote host.<br>**$reason:** Text describing what went wrong. |
| Log Error: 'Subscription $name: Failed to connect to $hostname ($ip): $error. | Critical. | **$name:** Log subscription name.<br>**$hostname:** Hostname of the syslog server.<br>**$ip:** IP address of the syslog server.<br>**$error:** Text of the error message. |

| Message | Alert Severity | Parameters |
|---|---|---|
| Log Error: Subscription $name: Network error while sending log data to syslog server $hostname ($ip): $error | Critical. | **$name:** Log subscription name.<br>**$hostname:** Hostname of the syslog server.<br>**$ip:** IP address of the syslog server.<br>**$error:** Text of the error message. |
| Subscription $name: Timed out after $timeout seconds sending data to syslog server $hostname ($ip). | Critical. | **$name:** Log subscription name.<br>**$timeout:** Timeout in seconds.<br>**$hostname:** Hostname of the syslog server.<br>**$ip:** IP address of the syslog server. |
| Subscription $name: Syslog server $hostname ($ip) is not accepting data fast enough. | Critical. | **$name:** Log subscription name.<br>**$hostname:** Hostname of the syslog server.<br>**$ip:** IP address of the syslog server. |
| Subscription $name: Oldest log file(s) were removed because log files reached the maximum number of $max_num_files. Files removed include:<br>$files_removed. | Information. | **$name:** Log subscription name.<br>**$max_num_files:** Maximum number of files allowed per log subscription.<br>**$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 '$report_title'.<br>This subscription should be examined and deleted if its configuration details are no longer valid. | Critical. | **$report_title:** Title of the report. |

| Message | Alert Severity | Parameters |
|---|---|---|
| A failure occurred while emailing periodic report '$report_title'.<br>This subscription has been removed from the scheduler. | Critical. | **$report_title:** Title of the report. |
| 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).<br>Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically. | Warning. | **$threshold:** Threshold value. |
| PERIODIC REPORTS: While building periodic report $report_title' the expected domain specification file could not be found at '$file_name'. No reports were sent. | Critical. | **$report_title:** Title of the report.<br>**$file_name:** Name of the file. |
| Counter group "$counter_group" does not exist. | Critical. | **$counter_group:** Name of the counter_group. |
| PERIODIC REPORTS: While building periodic report $report_title' the domain specification file '$file_name' was empty. No reports were sent. | Critical. | **$report_title:** Title of the report.<br>**$file_name:** Name of the file. |
| 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.<br>$error_text | Critical. | **$report_title:** Title of the report.<br>**$file_name:** Name of the file.<br>**$error_text:** List of errors encountered. |
| 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).<br>Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically. | Warning. | **$threshold:** Threshold value. |

| Message | Alert Severity | Parameters |
|---|---|---|
| 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.<br>The error message is:<br>$err_msg | Critical. | **$err_msg:** Error message text. |

## 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 $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage. | Warning. | **$app:** Web Security Appliance security service name.<br>**$attempts:** Number of attempts tried. |
| 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. |
| Certificate Revoke: OCSP validation failed for the UPDATER Server Certificate ($host:$port). Ensure the certificate is valid. | Critical | **$host:** The hostname of the UPDATER Server.<br>**$port:** The port of the UPDATER Server. |

## Anti-Malware Alerts

For information about alerts related to Advanced Malware Protection, see Ensuring That You Receive Alerts About Advanced Malware Protection Issues, on page 294.

## AMP Alerts

The following table contains a list of the various AMP alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

| Message | Alert Severity | Parameters |
|---|---|---|
| Appliance registration with AMP for Endpoints console failed.<br>$error | Warning | **$error:**Error message. |

| Message | Alert Severity | Parameters |
|---|---|---|
| Appliance ($devname) deregistration from AMP for Endpoints console failed.<br>$error | Warning | **$devname:**Device name.<br>**$error:**Error message. |

## Web Proxy Alerts

The following table contains a list of the various web proxy alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

| Message | Alert Severity | Parameters |
|---|---|---|
| An error occurred during disk read/write operation.<br>$error | Information | **$info:**Additional information such as object, object size being written. |
| The Web Proxy has detected that the contents of the caching partition are invalid. Flushing the cache might resolve the issue:<br>$errorstring | Information | **$errorstring:** Additional information as to why the cache content was invalid. |
| Configuration parameter errors.<br>$errorstring | Warning | **$errorstring:** A detailed description of the parameter value errors including both the parameter and its value. |
| Total client-side connections have exceeded threshold limit. Persistent connections are temporarily disabled.<br>$info | Warning | **$info:** Additional information. |
| The configured WCCPv2 Router is unresponsive or unreachable.<br>$info | Warning | **$info:** Additional information. |
| The configured upstream forward proxy is unresponsive or unreachable.<br>$info | Warning | **$info:** Additional information. |
| The Web Proxy process is out of memory and has restarted<br>$info | Warning | **$info:** Additional information. |
| An error occurred within the snmp library.<br>$info | Warning | **$info:** Additional information such as the snmp request in question. |
| Miscellaneous errors have caused the Web Proxy to exit.<br>$info | Warning | **$info:** Additional information if any. |

| Message | Alert Severity | Parameters |
|---|---|---|
| The DNS process has exited.<br>$info | Warning | **$info:** Additional information if any. |
| The authentication process has exited.<br>$info | Warning | **$info:** Additional information if any. |
| The Web Proxy was unable to reserve memory for major internal data structures during process startup.<br>$info | Critical | **$info:**Additional information such as size of various major internal data structures. |
| An error occurred during disk read/write operation.<br>$info | Critical | **$info:**Additional information such as object, object size being written. |

## External URL Categories Alerts

The following table contains a list of the various External URL Categries alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

| Message | Alert Severity | Parameters |
|---|---|---|
| $errmsg | Warning | **$errmsg:** Error message. |
| $errmsg | Information | **$errmsg:** Error message. |
| $errmsg | Critical | **$errmsg:** Error message. |

## L4 Traffic Monitor Alerts

The following table contains a list of the various L4 tarffic monitor alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

| Message | Alert Severity | Parameters |
|---|---|---|
| $errmsg | Warning | **$errmsg:** Error message. |
| $errmsg | Information | **$errmsg:** Error message. |
| $errmsg | Critical | **$errmsg:** Error message. |

## Policy Expiration Alerts

The following table contains a list of the various Policy Expiration alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

| Message | Alert Severity | Parameters |
|---|---|---|
| '$PolicyType': '$GroupName' has been disbaled due to expiry configuration. | Information | **$PolicyType:** Access policy / decryption policy based on the web policy type.<br>**$GroupName:**Policy group name. |
| '$PolicyType' : '$GroupName' will expire in days : 3. | Information | **$PolicyType:** Access policy / decryption policy based on the web policy type.<br>**$GroupName:** Policy group name. |

# 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 for use when no voluntary standards exist to meet federal requirements.

The Web Security Appliance achieves FIPS 140-2 compliance in FIPS mode using Cisco Common Cryptographic Module (C3M). By default, FIPS mode is disabled.

**Note** **From the AsyncOS 15.0 release onwards, the Federal Information Processing Standards (FIPS) mode is not supported.**

### Related Topics

- FIPS Mode Problems, on page 556

# 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
- Secure ICAP External DLP Configuration
- Identity Services Engine
- SSL Configuration
- SSH Configuration

**Note** The Appliance Management HTTPS Service must be configured with a FIPS Complaint certificate before FIPS mode can be enabled. The other encryption services need not be enabled.

A FIPS-compliant certificate must meet these requirements:

| Certificate | Algorithm | Signature Algorithm | Notes |
|---|---|---|---|
| X509 | RSA | sha1WithRSAEncryption<br>sha256WithRSAEncryption | 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. |

# FIPS Certificate Validation

When you enable FIPS mode, the appliance performs the following certificate checks:

- All certificates uploaded to the Web Security Appliance , whether by means of the UI or the `certconfig` CLI command, are validated to comply strictly with CC standards. Any certificate without a proper trust path in the Web Security Appliance 's trust store cannot be uploaded.
- Certificate Signature with a trusted path validation; Certificate/Public Key tampering with `basicConstrains` and `CAFlag` set validated for all signer certificates.
- OCSP validation is available to validate a certificate against a revocation list. This is configurable using the `certconfig` CLI command.

See also Strict Certificate Validation, on page 534.

# Enabling or Disabling FIPS Mode

### Before you begin

- Make a back-up copy of the appliance configuration; see Saving the Appliance Configuration File, on page 490
- Ensure the certificates to be used in FIPS mode use FIPS 140-2 approved public key algorithms (see FIPS Certificate Requirements, on page 529).

**Note**

- Changing the FIPS mode initiates a reboot of the appliance.
- When you disable FIPS mode, the SSL and SSH settings—which were automatically made FIPS-compliant when FIPS mode was enabled—are not reset to their default values. You must explicitly change these settings if you wish to allow a client using weaker SSH/SSL settings to connect. See SSL Configuration , on page 532 for additional information.

**Procedure**

**Step 1** Choose **System Administration** > **FIPS Mode**.

**Step 2** Click **Edit Settings**.

**Step 3** Check **Enable FIPS Compliance** to enable FIPS compliance.

When you check Enable FIPS Compliance, the **Enable encryption of Critical Sensitive Parameters (CSP)** check box is enabled.

**Step 4** Check **Enable encryption of Critical Sensitive Parameters (CSP)** to enable encryption of configuration data such as passwords, authentication information, certificates, shared keys, and so on.

**Step 5** Click **Submit**.

**Step 6** Click **Continue** to allow the appliance to reboot.

# System Date and Time Management


- Setting the Time Zone, on page 531
- Synchronizing the System Clock with an NTP Server , on page 531


## Setting the Time Zone

**Procedure**

**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

Cisco recommends that you set your Web Security Appliance to track the current date and time by querying a Network Time Protocol (NTP) server, not by manually setting the time on the appliance. This is especially true if your appliance integrates with other devices. All integrated devices should use the same NTP server.

**Procedure**

**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.

# SSL Configuration

For enhanced security, you can enable and disable SSL v3 and various versions of TLS for several services. Disabling SSL v3 for all services is recommended for best security. By default, all versions of TLS are enabled, and SSL is disabled.

**Note** You also can use the `sslconfig` CLI command to enable or disable these features. See Web Security Appliance CLI Commands, on page 591.

**Note** Restart the application when you modify or change the SSL configuration that results in disabling the TLS ciphers.

### Procedure

**Step 1** Choose **System Administration > SSL Configuration**.

**Step 2** Click **Edit Settings**.

**Step 3** Check the corresponding boxes to enable SSL v3 and TLS v1.x for these services:

- **Appliance Management Web User Interface** – Changing this setting will disconnect all active user connections.

  **Note**
  - For protocol versions, TLSv1.2 is enabled by default. You can now select TLSv1.3 by checking the TLSv1.3 checkbox or using the `sslconfig` command. Fore more details on the command, see Web Security Appliance CLI Commands, on page 591. If you are selecting TLSv1.3 as the protocol versions, it is mandatory to provide ciphers to use it.

- **Proxy Services** – Includes HTTPS Proxy and Credential Encryption for Secure Client. This section also includes:
  - **Cipher(s) to Use** – You can enter additional cipher suites to be used with Proxy Services communications. Use colons (:) to separate the suites. To prevent use of a particular cipher, add an exclamation point (!) to the front of that string. For example, `!EXP-DHE-RSA-DES-CBC-SHA` .

    Be sure to enter only suites appropriate to the TLS/SSL versions you have checked. Refer to https://www.openssl.org/docs/manmaster/man1/ciphers.html for additional information, and cipher lists.

The appliance supports TLSv1.3 version. Cipher `TLS_AES_256_GCM_SHA384` is added to the default cipher list. By default, TLSv1.3 is enabled on the appliance.

The default cipher for AsyncOS versions 9.0 and earlier is `DEFAULT:+kEDH`.

The default cipher for AsyncOS versions 9.1 - 11.8 is:

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
!AES256-SHA:DHE-RSA-AES128-SHA
```

In this case, the default cipher may change based on your ECDHE cipher selections.

The default cipher for AsyncOS versions 12.0 and later is:

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

**Note**
Update the default cipher suite while upgrading to a newer AsyncOS version. The ciphers suites are not automatically updated. When you upgrade from an earlier version to AsyncOS 12.0 and later, Cisco recommends updating the cipher suite to:

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

- **Disable TLS Compression (Recommended)** – You can check this box to disable TLS compression; this is recommended for best security.

- **Secure LDAP Services** – Includes Authentication, External Authentication and Secure Mobility.
- **Secure ICAP Services (External DLP)** – Select the protocol(s) used to secure ICAP communications between the appliance and external DLP (data loss prevention) servers. See Configuring External DLP Servers, on page 321 for more information.
- **Update Service** – Select the protocol(s) used for communications between the appliance and available update servers. See AsyncOS for Web Upgrades and Updates, on page 538 for more information about update services.

**Note**
Cisco's Update servers do not support SSL v3, therefore TLS 1.0 or above must be enabled for the Cisco Update service. However, SSL v3 can still be used with a local update server, if it is so configured—you must determine which versions of SSL/TLS are supported on that server.

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

# Certificate Management

The appliance uses digital certificates to establish, confirm and secure a variety of connections. The Certificate Management page lets you view and update current certificate lists, manage trusted root certificates, and view blocked certificates.

**Note** The Certificate Management page takes a long time to load and results in a timed-out error when the appliance is not connected to the internet. In addition, the "Failed to fetch manifest" network error is displayed in the Certificate Updates list after loading the certificate.

### Related Topics


- About Certificates and Keys, on page 534
- Certificate Updates, on page 535
- Managing Trusted Root Certificates, on page 535
- Viewing Blocked Certificates, on page 536


# Strict Certificate Validation

With the release of the FIPS-mode updates in AsyncOS 10.5, all presented certificates are validated strictly to comply with Common Criteria (CC) standards before uploading, and OCSP validation is available to validate certificates against a revocation list.

You must ensure that proper, valid certificates are uploaded to the Web Security Appliance , and that valid, secure certificates are configured on all related servers to facilitate smooth SSL handshakes with those servers.

Strict certificate validation is applied for the following certificate uploads:

- HTTPS Proxy (Security Services > HTTPS Proxy)
- File Analysis Server (Security Services > Anti-Malware and Reputation > Advanced Settings for File Analysis > File Analysis Server: Private Cloud & Certificate Authority: Use Uploaded Certificate Authority)
- Trusted Root Certificates (Network > Certificate Management)
- Global Authentication Settings (Network > Authentication > Global Authentication Settings)
- Identity Provider for SaaS (Network > Identity Provider for SaaS)
- Identity Services Engine (Network > Identity Services Engine)
- External DLP Servers (Network > External DLP Servers)
- LDAP & Secure LDAP (Network > Authentication > Realm)

See also FIPS Compliance, on page 529.

# About Certificates and Keys

When a browser prompts its user to authenticate, the browser sends the authentication credentials to the Web Proxy using a secure HTTPS connection. By default, the Web Security Appliance  uses the “Cisco Web Security Appliance Demo Certificate” that comes with it to create an HTTPS connection with the client. 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 that your applications recognize automatically.

### Related Topics

- Uploading or Generating a Certificate and Key, on page 536
- Certificate Signing Requests, on page 537
- Intermediate Certificates, on page 538

# Managing 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 primary list, it allows you to override trust in a certificate, which functionally removes the certificate from the trusted list.

To add, override or download a trusted root certificate:

### Procedure

**Step 1** Choose **Network** > **Certificate Management**.

**Step 2** Click **Manage Trusted Root Certificates** on the Certificate Management page.

**Step 3** To add a custom trusted root certificate with a signing authority not on the Cisco-recognized list:

Click **Import** and then browse to, select, and **Submit** the certificate file.

**Step 4** To override the trust for one or more Cisco-recognized certificates:

a) Check the **Override Trust** checkbox for each entry you wish to override.
b) Click **Submit**.

**Step 5** To download a copy of a particular certificate:

a) Click the name of the certificate in the Cisco Trusted Root Certificate List to expand that entry.
b) Click **Download Certificate**.

# Certificate Updates

The Updates section lists version and last-updated information for the Cisco trusted-root-certificate and blocked list bundles on the appliance. These bundles are updated periodically.

### Procedure

Click **Update Now** on the Certificate Management page to update all bundles for which updates are available.

# Viewing Blocked Certificates

To view a list of certificates which Cisco has determined to be invalid, and has blocked:

**Procedure**

Click **View Blocked Certificates**.

# Uploading or Generating a Certificate and Key

Certain AsyncOS features require a certificate and key to establish, confirm or secure a connection Identity Services Engine (ISE) and . You can either upload an existing certificate and key, or you can generate one when you configure the feature.

## Uploading a Certificate and Key

A 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.

**Procedure**

**Step 1** Select **Use Uploaded Certificate and Key**.

**Step 2** In the **Certificate** field, click Browse; locate the file to upload.

**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.

**Step 3** In the **Key** field, click Browse; locate the file to upload.

**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.

**Step 4** If the key is encrypted, select **Key is Encrypted**.

**Step 5** Click **Upload Files**.

# Generating a Certificate and Key

### Procedure

**Step 1** Select **Use Generated Certificate and Key**.

**Step 2** Click **Generate New Certificate and Key**.

a) In the Generate Certificate and Key dialog box, enter the necessary generation information.

**Note**
You can enter any ASCII character except the forward slash ( / ) in the Common Name field.

b) Click **Generate** in the Generate Certificate and Key dialog box.

When generation is complete, the certificate information is displayed in the Certificate section, along with two links: **Download Certificate** and **Download Certificate Signing Request**. In addition, there is a Signed Certificate option that is used to upload the signed certificate when you receive it from the Certificate Authority (CA).

**Step 3** Click **Download Certificate** to download the new certificate for upload to the appliance.

**Step 4** Click **Download Certificate Signing Request** to download the new certificate file for transmission to a Certificate Authority (CA) for signing. See Certificate Signing Requests, on page 537 for more information about this process.

a) When the CA returns the signed certificate, click Browse in the Signed Certificate portion of the Certificate field to locate the signed-certificate file, and then click Upload File to upload it to the appliance.

b) Ensure the CA's root certificate is present in the appliance's list of trusted root certificates. If it is not, add it. See Managing Trusted Root Certificates, on page 535 for more information.

# 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.

Servers send a "certificate chain" in an SSL handshake in order for clients (for example, browsers and in this case the Web Security Appliance , which is a HTTPS proxy) to authenticate the server. Normally, the server certificate is signed by an intermediate certificate which in turn is signed by a trusted root certificate, and during the handshake, the server certificate and the entire certificate chain are presented to the client. As the root certificate is typically present in the Trusted Certificate store of the Web Security Appliance , verification of the certificate chain is successful.

However, sometimes when the end-point entity certificate is changed on the server, necessary updates for the new chain are not performed. As a result, going forward the server presents only the server certificate during the SSL handshake and the Web Security Appliance proxy is unable to verify the certificate chain since the intermediate certificate is missing.

Previously, the solution was manual intervention by the Web Security Appliance administrator, who would upload the necessary intermediate certificate to the Trusted Certificate store. Now you can use the CLI command `advancedproxyconfig > HTTPS > Do you want to enable automatic discovery and download of missing Intermediate Certificates?` to enable "intermediate certificate discovery," a process the Web Security Appliance uses in an attempt to eliminate the manual step in these situations.

Intermediate certificate discovery uses a method called "AIA chasing": when presented with an untrusted certificate, the Web Security Appliance examines it for an extension named "Authority Information Access." This extension includes an optional CA Issuers URI field, which can be queried for the Issuer Certificate used to sign the server certificate in question. If it is available, the Web Security Appliance fetches the issuer's certificate recursively until the root CA certificate is obtained, and then tries to verify the chain again.

# 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, Loading, and Resetting the Appliance Configuration, on page 490

# Upgrading and Updating AsyncOS and Security Service Components

## Downloading and Installing an Upgrade

### Before you begin

Save the appliance configuration file (see Saving, Loading, and Resetting the Appliance Configuration, on page 490).

**Note** When downloading and upgrading AsyncOS in a single operation from a local server instead of from a Cisco server, the upgrade installs immediately while downloading. A banner is displayed for 10 seconds at the beginning of the upgrade process. While this banner is displayed, you can type Control-C to exit the upgrade process before downloading starts.

**Note** While performing an upgrade, if the secure authentication certificate is not FIPs-complaint, it will be replaced with the default certificate of the latest path to which your appliance is upgraded to. This happens only when the customer has used the default certificate before the upgrade.

You can download and install in a single operation, or download in the background and install later.

Upgrade fails if any configuration value stored in varstore files have non-ASCII characters.

### Procedure

**Step 1** Choose **System Administration** > **System Upgrade**.

**Step 2** Click **Upgrade Options**.

Select upgrade options and an upgrade image:

| Setting | Description |
|---|---|
| Choose an upgrade option | • **Download and install** – Download and install the upgrade in a single operation.<br>If you have already downloaded an installer, you will be prompted to overwrite the existing download.<br>• **Download only** – Download an upgrade installer, but do not install.<br>If you have already downloaded an installer, you will be prompted to overwrite the existing download. The installer downloads in the background without interrupting service.<br>An **Install** button is displayed when the download is complete; click to install a previously downloaded upgrade. |
| | Select an upgrade image to be downloaded, or downloaded and installed, from the **List of available upgrade images files at upgrade server**. |

| Setting | Description |
|---|---|
| Upgrade Preparation | • To save a back-up copy of the current configuration to the `configuration` directory on the appliance, check **Save the current configuration to the configuration directory before upgrading**.<br>• If the **Save current configuration** option is checked, you can check **Mask passwords in the configuration file** to have all current-configuration passwords masked in the back-up copy. However, you cannot load a configuration file with masked passwords using the **Load Configuration** command, nor with the CLI `loadconfig` command.<br>If FIPS mode is enabled, you can select **Encrypt passphrases in the Configuration Files**. These files can be reloaded.<br>• If the **Save current configuration** option is checked, you can enter one or more email addresses into the **Email file to** field; a copy of the back-up configuration file is mailed to each address. Separate multiple addresses with commas. |

**Step 3** Click **Proceed**.

If you are installing:

a) Be prepared to respond to prompts during the process.
b) At the completion prompt, click **Reboot Now**.
c) After about 10 minutes, access the appliance again and log in.

If you feel you need to power-cycle the appliance to troubleshoot an upgrade issue, do not do so until at least 20 minutes have passed since you rebooted.

## Viewing Status of, Canceling, or Deleting a Background Download

### Procedure

**Step 1** Choose **System Administration** > **System Upgrade**.

**Step 2** Click **Upgrade Options**.

**Step 3** Choose an option:

| To | Do This |
|---|---|
| View download status | Look in the middle of the page.<br>If there is no download in progress and no completed download waiting to be installed, you will not see download status information. |
| Cancel a download | Click the **Cancel Download** button in the middle of the page.<br>This option appears only while a download is in progress. |

| To | Do This |
|---|---|
| Delete a downloaded installer | Click the **Delete File** button in the middle of the page.<br>This option appears only if an installer has been downloaded. |

**Step 4** (Optional) View the Upgrade Logs.

### What to do next

### Related Topics

- Local And Remote Update Servers, on page 542

# 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, on page 546.

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 Updating and Upgrading from the Cisco Update Servers, on page 542.
   - **Local server.** For more information, see Upgrading from a Local Server, on page 543.

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 demand from the GUI pages related to the feature.

**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.

**Note** Updates that are in-progress cannot be interrupted. All in-progress updates must complete before new changes can be applied.

**Procedure**

**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.

The CLI and the Web application interface may be sluggish or unavailable during the update process.

# 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, on page 542.

**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.

### Procedure

**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.

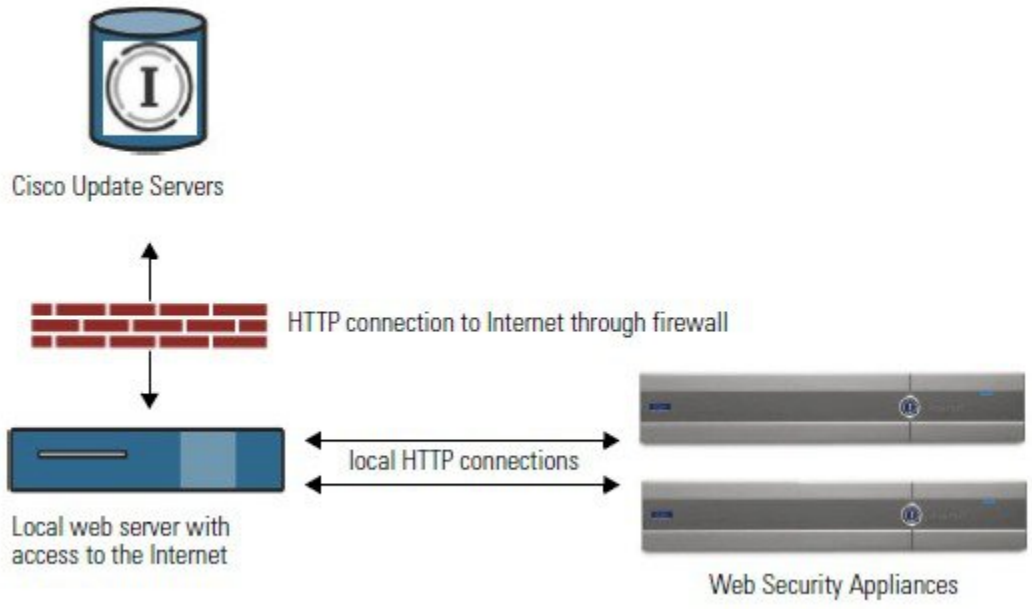
**Step 5** Submit and commit your changes.

## 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 Appliance s in your network.

The following figure shows how Web Security Appliance s download upgrade images from local servers.

***Figure 11: 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

**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.

### Procedure

**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.

## 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:

- The upgrading installs immediately *while downloading* .
- 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.

### Procedure

**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 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.<br>For more information, see AsyncOS for Web Upgrades and Updates, on page 538. |
| 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.<br>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 passphrase. |
| Update Servers (images) | Whether to download upgrade and update images from the Cisco update servers or a local web server.<br>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 passphrase. |
| 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 passphrase here. |

**Step 4** Submit and commit your changes.

### What to do next

### Related Topics

- Local And Remote Update Servers, on page 542

- Automatic and Manual Update and Upgrade Queries, on page 541
- Upgrading and Updating AsyncOS and Security Service Components, on page 539


# 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.

## Reverting AsyncOS on Virtual Appliances Impacts the License

If you revert to AsyncOS 8.0, there is no 180-day grace period during which the appliance processes web transactions without security features. License expiration dates are unaffected.

## 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 Primary Configuration 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

**Caution** 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.

**Caution** Smart Licensing configuration cannot be preserved if the operating system on a Secure Web Appliance is reverted to the previous version with Smart Licensing enabled. When you have successfully reverted to previous AsyncOS version, you should enable Smart Licensing and register it with the CSSM portal. If the **Specific/Permanent License Reservation** option was selected when Smart Software Licensing was activated, it is recommended to release the licenses used by the appliance before reverting the operation and de-register the appliance from CSSM portal. You can contact Cisco support for assistance if the licenses were not released or the appliance was not de-registered before the revert operation.

**Note** If updates to the set of URL categories are available, they will be applied after AsyncOS reversion.

### Before you begin

- Contact Cisco Quality Assurance to confirm that you can perform the intended reversion. (BS: this is a summary of the Available Versions section in the original topic. Have asked if this is correct.)
- Back up the following information from the Web Security Appliance to a separate machine:
  - System configuration file (with passphrases 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.

### Procedure

**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.

# Monitoring System Health and Status Using SNMP

The AsyncOS operating system supports system status monitoring via SNMP (Simple Network Management Protocol). (For more information about SNMP, see RFCs 1065, 1066, and 1067.)

Please note:

- SNMP is **off** by default.
- SNMP SET operations (configuration) are not implemented.
- AsyncOS supports SNMPv1, v2, and v3. For more information on SNMPv3, see RFCs 2571-2575.
- Message authentication and encryption are mandatory when enabling SNMPv3. Passphrases for authentication and encryption should be different. The encryption algorithm can be AES (recommended) or DES. The authentication algorithm can be SHA-1 (recommended) or MD5. The snmpconfig command "remembers" your passphrases 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 host name, but if you do, traps will only work if DNS is working.)

# MIB Files

MIB files are available from
http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

Use the latest version of each MIB file.

There are multiple MIB files:

- asyncoswebsecurityappliance-mib.txt — an SNMPv2 compatible description of the Enterprise MIB for Web Security Appliance s.

- ASYNCOS-MAIL-MIB.txt — an SNMPv2 compatible description of the Enterprise MIB for Email Security appliances.
- IRONPORT-SMI.txt — This "Structure of Management Information" file defines the role of the asyncoswebsecurityappliance-mib.

This release implements a read-only subset of MIB-II as defined in RFCs 1213 and 1907.

See https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.html to know about monitoring CPU usage on the appliance using SNMP.

# Enabling and Configuring SNMP Monitoring

To configure SNMP to gather system status information for the appliance, use the snmpconfig command in the command-line interface (CLI). After you choose and configure values for an interface, the appliance responds to SNMPv3 GET requests.

When you use SNMP monitoring, keep the following points in mind:

- These version 3 requests must include a matching passphrase.
- By default, version 1 and 2 requests are rejected.
- If enabled, version 1 and 2 requests must have a matching community string.

# Hardware Objects

Hardware sensors conforming to the Intelligent Platform Management Interface Specification (IPMI) report information such as temperature, fan speed, and power supply status.

To determine the hardware-related objects available for monitoring (for example, the number of fans or the operating temperature range), see the hardware guide for your appliance model.

### Related Topics

- Documentation Set, on page 613

# 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 ). After the condition has been met, the SNMP agent then forms an SNMP packet and sends it to the host running the SNMP management console software.

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.

### Related Topics

- About the connectivityFailure SNMP Trap , on page 550

## About the connectivityFailure SNMP Trap

The connectivityFailure trap is intended to monitor your appliance's connection to the internet. It does this by attempting to connect and send an HTTP GET request to a single external server every 5 to 7 seconds. By default, the monitored URL is `downloads.ironport.com` on port 80.

To change the monitored URL or port, run the `snmpconfig` command and enable the connecivityFailure trap, even if it is already enabled. You will see a prompt to change the URL.



**Tip** To simulate connectivityFailure traps, you can use the `dnsconfig` CLI command to enter a non-working DNS server. Lookups for downloads.ironport.com will fail, and traps will be sent every 5-7 seconds. Be sure to change the DNS server back to a working server after completing your test.

# CLI Example: snmpconfig

```
wsa.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?
[Y]>

Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: wsa.example.com)
[1]>

Which port shall the SNMP daemon listen on interface "Management"?
[161]>

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 authentication passphrase.
[]>

Please enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>

Please enter the SNMPv3 privacy passphrase again to confirm.
[]>

Service SNMP V1/V2c requests?
```

```
[N]> Y

Enter the SNMP V1/V2c community string.
[ironport]> public

Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>

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.
[127.0.0.1]> 203.0.113.1

Enter the Trap Community string.
[ironport]> tcomm

Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               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.
[]> 1,7,12

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]>

What threshold would you like to set for memory utilization?
[95]>

Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3

Enter the System Contact string.
[snmp@localhost]> wsa-admin@example.com

Current SNMP settings:
```

```
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: wsa-admin@example.com

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

wsa.example.com> commit

Please enter some comments describing your changes:
[]> Enable and configure SNMP

Changes committed: Fri Nov 06 18:13:16 2015 GMT
wsa.example.com>
```

# Web Traffic Tap

**Before You Begin:**Enabling Web Traffic Tap feature will result in reduced transaction handling capacity (requests per second) for the appliance as appliance will need additional CPU cycles and memory to copy the messages to the tap interface.

**Note** For reducing the performance impact due to Web Traffic Tap feature, reduce the amount of traffic that gets tapped by setting appropriate Web Traffic Tap policies.

This feature is not supported on Amazon Web Services (AWS)

Web Traffic Tap feature allows you to tap the HTTP and HTTPS web traffic that passes through the appliance and copy it to a Web Security Appliance  interface in-line with the real time data traffic. You can select the Web Security Appliance  interface to which the tapped traffic data is sent. If the tapped traffic includes HTTPS data, the appliance decrypts them based on the decryption policies before sending them to the tap interface. See Decryption Policies , on page 242.

The selected tap interface must be directly connected to an external security device for analysis, forensics, and archiving. Alternatively, it may be connected to a L2 switch on a dedicated VLAN.

**Note** The traffic mirrored on the tap interface is broadcast over Ethernet layer and not IP routable. Therefore a dedicated VLAN is required if connected to a L2 switch.

This feature also enables you to set Web Traffic Tap policies. Based on these customer defined policy filters, the appliance mirrors the web traffic that is available for the external security device. Web Traffic Tap feature provides visibility to the HTTPS traffic.

The term tapping refers to the reconstruction of complete TCP (Transmission Control Protocol) streams as if occurring between a directly connected client and server.

Virtual Web Security Appliance s support Web Traffic Tap feature.

**Note** The act of inspecting SSL traffic might be subject to corporate policy guidelines and/or national legislation. Cisco is not responsible for any legal obligations and it is your sole responsibility to ensure that your use of Web Traffic Tap feature on Web Security Appliance is in accordance with any such legal or policy requirements.

You must perform the following procedures to tap the web traffic using the appliance:

1. Enable Web Traffic Tap feature
2. Configure Web Traffic Tap policies

### Related Topics

- Enabling Web Traffic Tap, on page 553
- Configuring Web Traffic Tap Policies, on page 554

# Enabling Web Traffic Tap

### Before you begin

The Web Traffic Tap feature is disabled by default. You must enable the feature before you define the Web Traffic Tap policies using **Web Security Manager** > **Web Traffic Tap Policies**.

**Note** Decryption policies must be defined in order to tap HTTPS transactions. See Decryption Policies , on page 242.

### Procedure

**Step 1** Choose **Network** > **Web Traffic Tap**.

**Step 2** Click **Edit Settings**.

**Step 3** In the Edit Web Traffic Tap page, check the **Enable** check box to enable Web Traffic Tap feature.

**Note**
To disable the Web Traffic Tap feature, uncheck the **Enable** check box. If you disable the Web Traffic Tap feature, you will not be able to view or edit the Web Traffic Tap policies. You must enable the feature again to view and edit the policies.

**Step 4** From the Tap Interface drop-down list, choose the Web Security Appliance interface to which the tapped traffic data is sent. The interface options are P1, P2, T1, and T2. See Connect the Appliance, on page 11 to know about interfaces.

**Note**
The selected tap interface must be directly connected to an external security device for analysis, forensics, and archiving. Alternatively, it may be connected to a L2 switch on a dedicated VLAN. The tap interface chosen should be connected and its status should be active; if not, mirroring of tapped traffic will fail.

**Step 5** Click **Submit** and commit your changes.

# Configuring Web Traffic Tap Policies

### Procedure

**Step 1** Choose **Web Security Manager** > **Web Traffic Tap Policies**.

**Step 2** Click **Add Policy**.

Follow the instructions in Creating a Policy , on page 219to add a new Web Traffic Tap policy.

**Note**
A Global Traffic Tap policy with no tapping set is available by default on the Web Traffic Tap Policies page (**Web Security Manager** > **Web Traffic Tap Policies**).

**Step 3** Expand the Advanced section of the Policy Member Definition area to add the following additional group membership criteria for Web Traffic Tap.

- Protocols - Choose either HTTP or HTTPS protocol or both of them to create Web Traffic Tap Policy.

  **Note**
  You must define matching decryption policy (**Web Security Manager** > **Decryption Policies**) in order to tap HTTPS traffic.

  Web Traffic Tap policies do not support Native FTP and SOCKS protocols.

- Subnets
- URL Categories – Set **Tap** or **No Tap** for the URL Filtering categories as required. To set traffic tap for uncategorized URLs, choose **Tap** from the Uncategorized URLs drop-down list and click **Submit**.
- User Agents

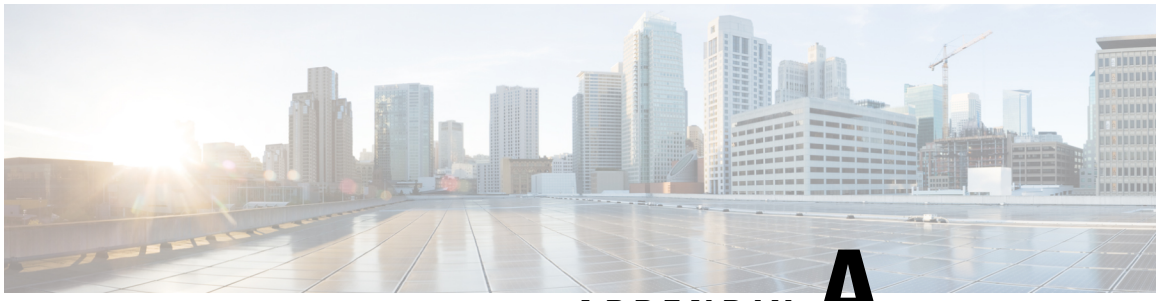
See Creating a Policy , on page 219 to know more about defining additional group membership criteria.

**Note**
The traffic that you want to tap must satisfy all the filter conditions that you have defined for the Web Traffic Tap policy.

You can also add URL categories from the URL Filtering table using **Web Security Manager** > **Web Traffic Tap Policies**.

**Note**
If you have already added the URL categories in the Advanced section, you will see only those URL categories listed in the URL Filtering table (**Web Security Manager** > **Web Traffic Tap Policies**).

See Policy Order, on page 218 to know about the Web Traffic Tap policy order.



APPENDIX A

# Troubleshooting

This topic contains the following sections:


- General Troubleshooting Best Practices, on page 555
- FIPS Mode Problems, on page 556
- Authentication Problems, on page 556
- Blocked Object Problems, on page 558
- Browser Problems, on page 559
- DNS Problems, on page 559
- Failover Problems, on page 559
- Feature Keys Expired, on page 560
- FTP Problems, on page 560
- Upload/Download Speed Issues, on page 561
- Hardware Issues, on page 562
- HTTPS/Decryption/Certificate Problems, on page 563
- Identity Services Engine Problems, on page 565
- Problems with Custom and External URL Categories, on page 568
- Logging Problems, on page 570
- Policy Problems, on page 571
- Problems with File Reputation and File Analysis , on page 577
- Reboot Issues, on page 577
- Site Access Problems, on page 578
- Upstream Proxy Problems, on page 579
- Virtual Appliances , on page 580
- WCCP Problems, on page 581
- Packet Capture, on page 581
- Working With Support , on page 583


## General Troubleshooting Best Practices

Configure your Access Logs to include the following custom fields:

%u, %g, %m, %k, %L (These values are case-sensitive.)

For descriptions of these fields, see Access Log Format Specifiers and W3C Log File Fields, on page 465.

For configuration instructions, see Customizing Access Logs, on page 460 and Adding and Editing Log Subscriptions, on page 432.

# FIPS Mode Problems

Check the following topics if you encounter encryption and certificate problems after you upgraded your Web Security Appliance to AsyncOS 10.5, and enabled FIPS mode and CSP encryption.

- CSP Encryption, on page 556
- Certificate Validation, on page 556

## CSP Encryption

For a feature that worked before you enabled FIPS-mode CSP encryption, but doesn't work after encryption is enabled, determine if the CSP encryption is the problem. Disable CSP encryption and FIPS mode and then test the feature. If it works, enable FIPS mode and test it again. If it works, enable CSP encryption and test it again. See Enabling or Disabling FIPS Mode , on page 530.

## Certificate Validation

Certificates which were accepted by your Web Security Appliance prior to upgrading to AsyncOS 10.5 might be rejected when they are uploaded again, regardless of upload method. (That is, via UI pages such as HTTPS Proxy, Certificate Management, Identity Provider for SaaS, ISE configuration, Authentication configuration, or via the `certconfig` CLI command.)

Ensure that the certificate's signer CAs have been added as "Custom Trusted Certificate Authorities" on the Certificate Management page (Network > Certificate Management). A certificate cannot be uploaded to the Web Security Appliance if the complete certificate path is untrusted.

Also, when reloading an older configuration, its likely that the included certificates will not be trusted and the reload will fail. Ensure these certificates are replaced while loading the saved configuration.

**Note** All certificate validation failures are logged in the audit logs (`/data/pub/audit_logs/audit_log.current`).

# Authentication Problems

- Troubleshooting Tools for Authentication Issues , on page 557
- Failed Authentication Impacts Normal Operations, on page 557
- LDAP Problems, on page 557
- Basic Authentication Problems, on page 558
- Single Sign-On Problems, on page 558
- Also see:
  - General Troubleshooting Best Practices, on page 555
  - HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 572

• Cannot Access URLs that Do Not Support Authentication, on page 578
• Client Requests Fail Upstream Proxy, on page 579

# Troubleshooting Tools for Authentication Issues

KerbTray or klist (both part of the Windows Server Resources Kit) for viewing and purging a Kerberos ticket cache. Active Directory Explorer for viewing and editing an Active directory. Wireshark is a packet analyzer you can use for network troubleshooting.

# Failed Authentication Impacts Normal Operations

When certain user agents or applications fail to authenticate and are denied access, they repeatedly send requests to the Web Security Appliance , which in turn repeatedly sends requests to the Active Directory servers with machine credentials, sometimes to the point of impacting normal operations.

For best results, bypass authentication with these user agents. See Bypassing Authentication with Problematic User Agents , on page 120.

# LDAP Problems

• LDAP User Fails Authentication due to NTLMSSP, on page 557
• LDAP Authentication Fails due to LDAP Referral, on page 557

## 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 Identification Profile uses a sequence that contains both LDAP and NTLM realms.
- The Identification Profile uses the “Basic or NTLMSSP” authentication scheme.
- A user sends a request from an application that chooses NTLMSSP over Basic.

Reconfigure the Identification Profile 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, on page 558

**Related Problems**

- Upstream Proxy Does Not Receive Basic Credentials, on page 579

## Basic Authentication Fails

AsyncOS for Web only supports 7-bit ASCII characters for passphrases when using the Basic authentication scheme. Basic authentication fails when the passphrase contains characters that are not 7-bit ASCII.

# Single Sign-On Problems

- Users Erroneously Prompted for Credentials, on page 558

## 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).

# Blocked Object Problems

- Some Microsoft Office Files Not Blocked, on page 558
- Blocking DOS Executable Object Types Blocks Updates for Windows OneCare, on page 559

# 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.

# Browser Problems

• WPAD Not Working With Firefox, on page 559

## 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.

### Procedure

**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, on page 559

## 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.

# Failover Problems

• Failover Misconfiguration, on page 560
• Failover Issues on Virtual Appliances , on page 560

## Failover Misconfiguration

Misconfiguration of failover groups might result in multiple primary appliances or other failover problems. Diagnose failover problems using the `testfailovergroup` subcommand of the CLI `failoverconfig` command.

For example:

```
wsa.wga> failoverconfig
Currently configured failover profiles:
1.      Failover Group ID: 61
        Hostname: failoverV4P1.wga, Virtual IP: 10.4.28.93/28
        Priority: 100, Interval: 3 seconds
        Status: PRIMARY
Choose the operation you want to perform:
- NEW - Create new failover group.
- EDIT - Modify a failover group.
- DELETE - Remove a failover group.
- PREEMPTIVE - Configure whether failover is preemptive.
- TESTFAILOVERGROUP - Test configured failover profile(s)
[]> testfailovergroup
Failover group ID to test (-1 for all groups):
[]> 61
```

## Failover Issues on Virtual Appliances

For deployments on virtual appliances, ensure that you have configured the interface/ virtual switch on the hypervisor to use promiscuous mode.

# 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, on page 560
- Large FTP Transfers Disconnect, on page 561
- Zero Byte File Appears On FTP Servers After File Upload, on page 561
- Chrome Browser Not Detected As User Agent in FTP-over-HTTP Requests, on page 561
- Also see:
  - Unable to Route FTP Requests Via an Upstream Proxy, on page 580
  - HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 572


## 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 workaround 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.

## Chrome Browser Not Detected As User Agent in FTP-over-HTTP Requests

Chrome browsers do not include a user-agent string in FTP-over-HTTP requests; therefore, Chrome cannot be detected as the user agent in those requests.

# Upload/Download Speed Issues

The Web Security Appliance is designed to handle thousands of client and server connections in parallel, and the sizes of the send and receive buffers are configured to deliver optimal performance, without sacrificing stability. Generally, actual usage is browse traffic, consisting of numerous short-lived connections for which we have receive-packet-steering (RPS) and receive-flow-steering (RFS) data, and for which the Web Security Appliance has been optimized.

However, at times you may experience a noticeable reduction in upload or download speeds; for example, when transferring large files via proxy. To illustrate: assuming a 10-Mbps line, downloading a 100-MB file that passes through a Web Security Appliance can be approximately seven to eight times slower than downloading the file directly from its server.

In non-typical environments that include a larger proportion of large-file transfers, you can use the `networktuning` command to increase send and receive buffer size to alleviate this issue, but doing so can also cause network memory exhaustion and affect system stability. See Web Security Appliance CLI Commands, on page 591 for details of the `networktuning` command.



**Caution** Exercise care when changing the TCP receive and send buffer control points and other TCP buffer parameters. Use the `networktuning` command only if you understand the ramifications.

To configure the buffer size in `networktuning`, ensure that you have enabled the automatic send and receive options that are provided under `networktuning`.

Here are examples of using the `networktuning` command on two different appliances:

**On an S380**

```
networktuning
sendspace = 131072
recvspace = 131072
send-auto = 1 [Remember to disable miscellaneous > advancedproxy > send buf auto tuning]
recv-auto = 1 [Remember to disable miscellaneous > advancedproxy > recv buf auto tuning]
mbuf clusters = 98304 * (X/Y)  where is X is RAM in GBs on the system and Y is 4GB.
sendbuf-max = 1048576
recvbuf-max = 1048576
```

**Questions**

**What are these parameters?**

The Web Security Appliance has several buffers and optimization algorithms which can be altered for specific needs. Buffer sizes are originally optimized to suit the "most common" deployment scenarios. However, larger buffer sizes can be used when faster per-connection performance is needed, but note that overall memory usage will increase. Therefore, buffer-size increases should be in line with the memory available on the system. The send- and receive-space variables control the size of the buffers available for storing data for communication over a socket. The send- and receive-auto options are used to enable and disable dynamic scaling of send and receive TCP window sizes. (These parameters are applied in the FreeBSD kernel.)

**How were these example values determined?**

We tested different sets of values on a customer's network where this "problem" was observed, and "zeroed in" on these values. We then further tested these changes for stability and performance increase in our labs. You are free to use values other than these at your own risk.

**Why are these values not the defaults?**

As mentioned, by default the Web Security Appliance is optimized for the most-common deployments, and operating in a very large number of locations without per-connection performance complaints. Making the changes discussed here will not increase RPS numbers, and in fact may cause them to drop.

# Hardware Issues


- Cycling Appliance Power , on page 562
- Appliance Health and Status Indicators , on page 562
- Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware, on page 563


## Cycling Appliance Power

**Important!** If you need to cycle power to your x80 or x90 appliance, wait at least 20 minutes for the appliance to come up again (all LEDs are green) before pushing the power button.

## Appliance Health and Status Indicators

Lights on the front and/or rear panels of your hardware appliance indicate health and status of your appliance. For descriptions of these indicators, see the hardware guides, such as the *Cisco x90 Series Content Security Appliances Installation and Maintenance Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Specifications for your appliance, such as temperature ranges, are also available in these documents.

# Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware

This alert may or may not indicate a problem. The battery relearn timeout, in itself, does not mean there is any problem with the RAID controller. The controller can recover in the subsequent relearn. Please monitor your email for any other RAID alerts for the next 48 hours, to ensure that this is not the side-effect of any other problem. If you do not see any other RAID-type alerts from the system, then you can safely ignore this alert.

# HTTPS/Decryption/Certificate Problems


- Accessing HTTPS Sites Using Routing Policies with URL Category Criteria, on page 563
- HTTPS Request Failures, on page 563
- Bypassing Decryption for Particular Websites, on page 564
- Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content, on page 564
- Alert: Problem with Security Certificate, on page 565
- Also see:
  - Logging HTTPS Transactions, on page 570
  - Access Policy not Configurable for HTTPS, on page 571
  - HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 572


# 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 any user-defined Routing Policy because of insufficient information.

As a result, transparently redirected HTTPS transactions only match Routing Policies if no Routing Policy Group and no identification profile has a membership criteria. If any user-defined Routing Policies or identification profiles define their membership by URL category, then the transparent HTTPS transactions match the Default Routing Policy Group.

# HTTPS Request Failures


- HTTPS with IP-based Surrogates and Transparent Requests, on page 563
- Different Client “Hello” Behavior for Custom and Default Categories, on page 564


## 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 topic.

## Different Client "Hello" Behavior for Custom and Default Categories

When scanning packet captures, you may notice that the "Client Hello" handshake is sent at different times for custom category and default (Web) category HTTPS Decryption pass-through policies.

For an HTTPS page passed through via the default category, the Client Hello is sent before receipt of a Client Hello from the requestor, and the connection fails. For an HTTPS page passed through via a custom URL category, the Client Hello is sent after the Client Hello is received from the requestor, and the connection is successful.

As a remedy, you can create a custom URL category with a pass-through action for SSL 3.0-only-compatible Web pages.

# 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.

### Procedure

**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.

# Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content

Referrer-based exceptions are supported only in Access policies. To use this feature with HTTPS traffic, before defining exceptions in Access policies, you must configure HTTPS decryption of the URL Categories that you will select for exception. However, this feature will not work under certain conditions:



**Note** When time ranges are configured, they receive the highest priority. The referrer will not function if the Time Range quota has been reached.

- If the connection is tunneled and HTTPS decryption is not enabled, this feature will not work for requests going to HTTPS sites.
- According to RFC 2616, a browser client could have a toggle switch for browsing openly/anonymously, which would respectively enable/disable the sending of Referer and from information. The feature is exclusively dependent on the Referer header, and turning off sending them would cause our feature not to work.

- According to RFC 2616, clients should not include a Referer header field in a (non-secure) HTTP request if the referring page was transferred with a secure protocol. So, any request from an HTTPS-based site to an HTTP-based site would not have the Referer header, causing this feature to not work as expected.
- When a Decryption policy is set up such that when a custom category matches the Decryption policy and the action is set to Drop, any incoming request for that category will be dropped, and no bypassing will be done.

## 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.

# Identity Services Engine Problems


- Tools for Troubleshooting ISE Issues, on page 565
- ISE Server Connection Issues, on page 566
- ISE-related Critical Log Messages, on page 568


## Tools for Troubleshooting ISE Issues

The following can be useful when troubleshooting ISE-related issues:

- The ISE test utility, used to test the connection to the ISE server, provides valuable connection-related information. This is the **Start Test** option on the Identity Services Engine page; see Connect to the ISE/ISE-PIC Services, on page 155.
- ISE and Proxy Logs; see Monitor System Activity Through Logs, on page 425
- ISE-related CLI commands `iseconfig` and `isedata` , particularly `isedata` to confirm security group tag (SGT) download. See Web Security Appliance CLI Commands, on page 591 for additional information.
- The Web Tracking and Policy Trace functions can be used to debug policy match issues; for example, a user that should be allowed is blocked, and vice versa. See Policy Troubleshooting Tool: Policy Trace, on page 573 for additional information.
- Packet Capture, on page 581 if Working With Support , on page 583.

- For checking certificate status, you can use the openssl Online Certificate Status Protocol ( ocsp ) utility, available from https://www.openssl.org/ .

# ISE Server Connection Issues

## Certificate Issues

The Web Security Appliance and the ISE server(s) use certificates to mutually authenticate for successful connection. Thus, each certificate presented by one entity should be recognizable by other. For example, if the Web Security Appliance 's Client certificate is self-signed, the same certificate must be present in the trusted certificates list on the appropriate ISE server(s). Correspondingly, if the Web Appliance Client certificate is CA-signed, then the CA root certificate must be present on the appropriate ISE server(s). Similar requirements apply to the ISE server-related Admin and pxGrid certificates.

Certificate requirements and installation are described in Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service, on page 149. If you encounter certificate-related issues, check the following:

- If using CA-signed certificates:
  - Verify that the root CA signing certificate(s) for the Admin and pxGrid certificates are present on the Web Security Appliance .
  - Verify that the root CA signing certificate for the Web Appliance Client certificate is present in the trusted-certificates list on the ISE server.
- If using self-signed certificates:
  - Verify that the Web Appliance Client certificate—generated on the Web Security Appliance and downloaded—has been uploaded to the ISE server and is present in the ISE servers trusted-certificates list.
  - Verify that the ISE Admin and pxGrid certificates—generated on the ISE server and downloaded—have been uploaded to the Web Security Appliance are present in the its certificate list.
- Expired certificates:
  - Confirm that certificates which were valid when uploaded have not expired.

### Log Output Indicating Certificate Issue

The following ISE-service log snippet shows a client-connection timeout due to a missing or invalid certificate.

```
Tue Mar 24 03:56:14 2015 Debug: ISELoggerThread: Logging queue starting
Tue Mar 24 03:56:14 2015 Info: ISEService: Successfully loaded configuration from: /data/ise/ise_servi
Tue Mar 24 03:56:14 2015 Debug: Statistics loaded from file
Tue Mar 24 03:56:14 2015 Info: ISEService: RPC Server Socket :/tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: RPCServer: Starting at: /tmp/ise_fastrpc.sock
Tue Mar 24 03:56:14 2015 Info: ISEService: Running
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE client attempt 0
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Creating ISE connection with reconnection True
Tue Mar 24 03:56:14 2015 Info: ISEService: Sending ready signal...
Tue Mar 24 03:56:14 2015 Info: ISEDynamicConfigThread: Started Server..
Tue Mar 24 03:56:14 2015 Debug: ISEEngineManager: Successfully created ISE client
Tue Mar 24 03:56:14 2015 Trace: ISEEngineManager: Waiting for client connection, 0 seconds of 30
Tue Mar 24 03:56:17 2015 Trace: ISEEngineManager: Waiting for client connection, 3 seconds of 30
Tue Mar 24 03:56:20 2015 Trace: ISEEngineManager: Waiting for client connection, 6 seconds of 30
Tue Mar 24 03:56:23 2015 Trace: ISEEngineManager: Waiting for client connection, 9 seconds of 30
Tue Mar 24 03:56:26 2015 Trace: ISEEngineManager: Waiting for client connection, 12 seconds of 30
Tue Mar 24 03:56:29 2015 Trace: ISEEngineManager: Waiting for client connection, 15 seconds of 30
Tue Mar 24 03:56:32 2015 Trace: ISEEngineManager: Waiting for client connection, 18 seconds of 30
Tue Mar 24 03:56:35 2015 Trace: ISEEngineManager: Waiting for client connection, 21 seconds of 30
Tue Mar 24 03:56:38 2015 Trace: ISEEngineManager: Waiting for client connection, 24 seconds of 30
Tue Mar 24 03:56:41 2015 Trace: ISEEngineManager: Waiting for client connection, 27 seconds of 30
Tue Mar 24 03:56:44 2015 Trace: ISEEngineManager: Waiting for client connection, 30 seconds of 30
Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out
Tue Mar 24 03:56:47 2015 Debug: ISEEngineManager: Stopping client...
```

These Trace-level log entries on the Web Security Appliance  show that after 30 seconds the attempts to connect to the ISE server are terminated.

## Network Issues

If connection to the ISE server fails during the Start Test on the Identity Services Engine page (Connect to the ISE/ISE-PIC Services, on page 155), check connectivity to the configured ISE server on ports 443 and 5222.

Port 5222 is the official client-to-server Extensible Messaging and Presence Protocol (XMPP) port, and is used for connection to the ISE server; it is also used by applications such as Jabber and Google Talk. Note that some firewalls are configured to block port 5222.

Tools that can be used to check connectivity include `tcpdump`

## Other ISE Server Connectivity Issues

The following issues can cause failure when the Web Security Appliance  attempts to connect with the ISE server:

- Licenses on the ISE server have expired.
- The pxGrid node status is “not connected” on the ISE server’s Administration > pxGrid Services page. Be sure Enable Auto-Registration is selected on this page.
- Outdated Web Security Appliance  clients (specifically “test_client” or “pxgrid_client”) are present on the ISE server. These need to be deleted; see Administration > pxGrid Services > Clients on the ISE server.
- The Web Security Appliance  is attempting to connect to the ISE server before all its services are up and running.

Some changes on the ISE server, such as certificate updates, require the ISE server or services running on it to restart. Any attempt to connect to the ISE server during this time will fail; however, eventually the connection will succeed.

## ISE-related Critical Log Messages

This section contains explanations for ISE-related critical Log messages on the Web Security Appliance :

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Waiting for client connection timed out`

  The Web Security Appliance 's ISE process failed to connect to the ISE server for 30 seconds.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: WSA Client cert/key missing. Please check ISE config`

  The Web Appliance Client certificate and key were not uploaded or generated on the Web Security Appliance 's Identity Service Engine configuration page.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: ISE service exceeded maximum allowable disconnect duration with ISE server`

  The Web Security Appliance 's ISE process could not connect to the ISE server for 120 seconds and exited.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Subscription to updates failed ...`

  The Web Security Appliance 's ISE process could not subscribe to the ISE server for updates.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Could not create ISE client: ...`

  Internal error when creating the Web Security Appliance 's ISE client for ISE server connection.

- `Tue Mar 24 03:56:47 2015 Critical: ISEEngineManager: Bulk Download thread failed: ...`

  Internal error indicating bulk download of SGTs failed on connection or re-connection.

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to start service. Error: ...`

  The Web Security Appliance 's ISE service failed to start.

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send ready signal ...`

  The Web Security Appliance 's ISE service was unable to send a ready signal to heimdall .

- `Tue Mar 24 03:56:47 2015 Critical: ISEService: Unable to send restart signal ...`

  The Web Security Appliance 's ISE service was unable to send a restart signal to heimdall .

# Problems with Custom and External URL Categories

- Issues Downloading An External Live Feed File, on page 569
- MIME Type Issue on IIS Server for .CSV Files, on page 569
- Malformed Feed File Following Copy and Paste, on page 570

# Issues Downloading An External Live Feed File

When Creating and Editing Custom and External URL Categories and providing an **External Live Feed** file (either **Cisco Feed Format** or **Office 365 Feed Format**), you must click the **Get File** button to initiate connection to the specified server, and download and parsing of the file. Progress and results of this process are displayed; if errors occur they are described. Rectify the problems and try downloading the file again.

There are four types of possible error:

- Connect exceptions

  `Failed to resolve server hostname` – the URL provided as the feed-file location is invalid; provide a correct URL to resolve this issue.

- Protocol errors

  `Authentication failed due to invalid credentials` – Server authentication failed; provide the correct user name and passphrase for server connection.

  `The requested file is not found on the server` – The URL provided for the feed file points to an invalid resource. Ensure the correct file is available on the specified server.

- Content validation errors

  `Failed to validate the content of the field` – The content of the feed file is invalid.

- Parsing errors

  - The Cisco Feed Format .csv file must contain one or more entries, where each entry is a site address or a valid regex string, followed by a comma and then the addresstype (which can be either `site` or `regex`). If this convention is not followed for any entry in the feed file, a parsing error is thrown.

    Also, do not include `http://` or `https://` as part of any `site` entry in the file, or an error will occur. In other words, `www.example.com` is parsed correctly, while `http://www.example.com` produces an error.

  - The XML feed file obtained from a Microsoft server is parsed by a standard XML parser. Any inconsistencies in the XML tagging are also flagged as parsing errors.

  The line number of a parsing error is included in the log. For example:

  `Line 8: 'www.anyurl.com' - Line is missing address or address-type field.` Line 8 in the feed file doesn't include a valid address or regex pattern, or an addresstype.

  `Line 12: 'www.test.com' - Unknown address type.` Line 12 has a invalid addresstype; the addresstype can be either `site` or `regex`.

# MIME Type Issue on IIS Server for .CSV Files

When providing a .csv file for the **External Live Feed Category** > **Cisco Feed Format** option while Creating and Editing Custom and External URL Categories, you may encounter a "406 not acceptable" error when fetching the file if the Cisco Feed Format server is running Internet Information Services (IIS) version 7 or 8 software. Similarly, the `feedsd` log will report something like: `31 May 2016 16:47:22 (GMT +0200) Warning: Protocol Error: 'HTTP error while fetching file from the server'.`

This is because the default MIME type for .csv files on IIS is `application/csv` rather than `text/csv`. You can remedy the problem by logging into the IIS server and editing the MIME type entry for .csv files to be `text/csv`.

## Malformed Feed File Following Copy and Paste

If you copy and paste the contents of a .csv (text) feed file from a UNIX or OS X system to a Windows system, an extra carriage return (`\r`) is added automatically and this can make the feed file malformed.

If you manually create the .csv file, or if you transfer the file from a UNIX or OS X system to a Windows server using SCP, FTP, or POST, there should be no problem.

# Logging Problems


- Custom URL Categories Not Appearing in Access Log Entries, on page 570
- Logging HTTPS Transactions, on page 570
- Alert: Unable to Maintain the Rate of Data Being Generated, on page 570
- Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs, on page 571


## 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, on page 571
- Blocked Object Problems, on page 558
- Identification Profile Disappeared from Policy, on page 572
- Policy Match Failures, on page 572
- Policy Troubleshooting Tool: Policy Trace, on page 573
- Also see: Accessing HTTPS Sites Using Routing Policies with URL Category Criteria, on page 563


## 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, on page 558
- Blocking DOS Executable Object Types Blocks Updates for Windows OneCare, on page 559

### 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.

## Identification Profile Disappeared from Policy

Disabling an Identification Profile removes it from associated policies. Verify that the Identification Profile is enabled and then add it to the policy again.

## Policy Match Failures

- Policy is Never Applied, on page 572
- HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, on page 572
- User Matches Global Policy for HTTPS and FTP over HTTP Requests, on page 573
- User Assigned Incorrect Access Policy , on page 573

### Policy is Never Applied

If multiple Identification Profiles have identical criteria, AsyncOS assigns the transactions to the first Identification Profile that matches. Therefore, transactions never match the additional, identical Identification Profiles, and any policies that apply to those subsequent, identical Identification Profiles 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 Identification Profile according to the other membership criteria, but the Web Proxy does not prompt clients for authentication even if the Identification Profile 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.
- Identification Profile 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.

### Procedure

**Step 1** Use the `advancedproxyconfig > authentication` CLI command.

**Step 2** Enter the surrogate timeout for machine credentials.

## Policy Trace Mismatch after Modifying Policy Parameters

When you modify policy parameters such as Access Policy, Identification Profiles and Users, Select One or More Identification Profiles, or Selected Groups and Users, the changes will take a few minutes to take effect.

# Policy Troubleshooting Tool: Policy Trace

- About the Policy Trace Tool, on page 574
- Tracing Client Requests, on page 574
- Advanced: Request Details, on page 575
- Advanced: Response Detail Overrides, on page 576

# 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 can perform a basic trace, or you can enter advanced trace settings and override options.

**Note** When you use the Policy Trace tool, the Web Proxy does not record the requests in the access log or reporting database.

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.

# Tracing Client Requests

**Note** You can use the CLI command `maxhttpheadersize` to change the maximum HTTP header size for proxy requests. Increasing this value can alleviate Policy Trace failures that can occur when the specified user belongs to a large number of authentication groups, or when the response header is larger than the current maximum header size. See Web Security Appliance CLI Commands, on page 591 for more information about this command.

### Procedure

**Step 1** Choose **System Administration > Policy Trace**.

**Step 2** Enter the URL you wish to trace to in the Destination URL field.

**Step 3** (Optional) Enter additional emulation parameters:

| To emulate... | Enter... |
|---|---|
| The client source IP used to make the request. | An IP address in the Client IP Address field.<br>**Note**<br>If an IP address is not specified, AsyncOS uses localhost. Also, SGTs (security group tags) cannot be fetched and policies based on SGTs will not be matched. |

| To emulate... | Enter... |
|---|---|
| The authentication/identification credentials used to make the request. | A user name in the User Name field, and then choose Identity Services Engine or an authentication realm from the Authentication/Identification drop-down list.<br>**Note**<br>Only enabled option(s) are available. That is, authentication options and the ISE option are available only if they are both enabled.<br>For authentication of 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.

**Note**
For a Pass Through HTTPS transaction, the Policy Trace tool bypasses further scanning and no Access policy is associated with the transaction. Similarly, for a Decrypt HTTPS transaction, the tool cannot actually decrypt the transaction to determine the applied Access policy. In both cases, as well as for Drop transactions, the trace results display: “Access policy: Not Applicable.”

**Note**
If the client IP address provided is not routable, the trace results display: "Connection Trace: Connection to Origin Server: Failed".

### What to do next

### Related Topics

- Advanced: Request Details, on page 575
- Advanced: Response Detail Overrides, on page 576

## Advanced: Request Details

You can use the settings in the Request Details pane of the Policy Trace page, Advanced section, to tune the outbound malware scan request for this policy trace.

### Procedure

**Step 1** Expand the **Advanced** section on the Policy Trace page.

**Step 2** Complete the fields in the Request Details pane as required:

| Setting | Description |
|---|---|
| Proxy Port | Select a specific proxy port to use for the trace request to test policy membership based on proxy port. |
| User Agent | Specify the User Agent to simulate in the request. |

| Setting | Description |
|---|---|
| Time of Request | Specify the Date and Time of day to simulate in the request. |
| Upload File | Choose a local file to simulate uploading in the request.<br>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 | To override a Webroot, McAfee, or Sophos scanning verdict, choose the specific type of verdict to be overridden. |

**Step 3** Click **Find Policy Match.**

The Policy Trace output is displayed in the Results pane.

## Advanced: Response Detail Overrides

You can use the settings in the Response Detail Overrides pane of the Policy Trace page, Advanced section, to “tweak” aspects of the Web Access Policies response for this trace.

### Procedure

**Step 1** Expand the **Advanced** section on the Policy Trace page.

**Step 2** Complete the fields in the Response Detail Overrides pane as required:

| Setting | Description |
|---|---|
| URL Category | Use this setting to override the URL transaction category of the trace response. Choose a category which is to replace the URL category in the response results. |
| Application | Similarly, use this setting to override the application category of the trace response. Choose a category which is to replace the application category in the response results. |
| Object Size | Enter a size for the response object in bytes. You can enter K, M, or G to represent Kilobytes, Megabytes, or Gigabytes. |
| MIME Type | Enter a MIME type. |
| Web Reputation Score | Enter a web reputation score from -10.0 to 10.0.<br>The web reputation score -100 means 'No Score.' |
| Anti-malware Scanning Verdicts | Use these options to override specific anti-malware scanning verdicts provided in the trace response. Choose verdicts which are to replace the Webroot, McAfee, and Sophos scanning verdicts in the response results. |

**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 , on page 299

# Reboot Issues


- Virtual Appliance Running on KVM Hangs on Reboot , on page 577
- Hardware Appliances: Remotely Resetting Appliance Power , on page 577


## Virtual Appliance Running on KVM Hangs on Reboot

**Note** This is a KVM issue and may change at any time.

For more information, see https://www.mail-archive.com/kvm@vger.kernel.org/msg103854.html and https://bugs.launchpad.net/qemu/+bug/1329956.

### Procedure

**Step 1** Check the following:

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

**Step 2** If the above value is set to Y:

a) Stop your virtual appliances and reinstall the KVM kernel module:

```
rmmod kvm_intel  modprobe kvm_intel enable_apicv=N
```

b) Restart your virtual appliance.

## Hardware Appliances: Remotely Resetting Appliance Power

### Before you begin

- Obtain and set up a utility that can manage devices using IPMI version 2.0.
- Understand how to use the supported IPMI commands. See the documentation for your IPMI tool.

If a hardware appliance requires a hard reset, you can reboot the appliance chassis remotely using a third-party Intelligent Platform Management Interface (IPMI) tool.

### Restrictions

- Remote power cycling is available only on certain hardware. For specifics, see Enabling Remote Power Cycling , on page 508.
- If you want be able to use this feature, you must enable it in advance, before you need to use it. For details, see Enabling Remote Power Cycling , on page 508.
- Only the following IPMI commands are supported: status, on, off, cycle, reset, diag, soft. Issuing unsupported commands will produce an “insufficient privileges” error.

**Procedure**

**Step 1** Use IPMI to issue a supported power-cycling command to the IP address assigned to the Remote Power Cycle port, which you configured earlier, along with the required credentials.

For example, from a UNIX-type machine with IPMI support, you might issue the command:

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

For S195, S395, and S695 models, use :

```
ipmitool -I lanplus -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

where `192.0.2.1` is the IP address assigned to the Remote Power Cycle port and remoteresetuser and passphrase are the credentials that you entered while enabling this feature.

**Step 2** Wait at least eleven minutes for the appliance to reboot.

# Site Access Problems

- Cannot Access URLs that Do Not Support Authentication, on page 578
- Cannot Access Sites With POST Requests , on page 579
- Also see: Bypassing Decryption for Particular Websites, on page 564

## 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, on page 121

## 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 a 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, on page 121.

# Upstream Proxy Problems

- Upstream Proxy Does Not Receive Basic Credentials, on page 579
- Client Requests Fail Upstream Proxy, on page 579

## 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.

# Virtual Appliances


- Do Not Use Force Reset, Power Off, or Reset Options During AsyncOS Startup , on page 580
- Network Connectivity on KVM Deployments Works Initially, Then Fails , on page 580
- Slow Performance, Watchdog Issues, and High CPU Usage on KVM Deployments , on page 580
- General Troubleshooting for Virtual Appliances Running on Linux Hosts , on page 580


## Do Not Use Force Reset, Power Off, or Reset Options During AsyncOS Startup

The following actions on your virtual host are the equivalent of pulling the plug on a hardware appliance and are not supported, especially during AsyncOS startup:

- In KVM, the Force Reset option.
- In VMWare, the Power Off and Reset options. (These options are safe to use after the appliance has come up completely.)

## Network Connectivity on KVM Deployments Works Initially, Then Fails

**Problem**

Network connectivity is lost after previously working.

**Solution**

This is a KVM issue. See the section on "KVM: Network connectivity works initially, then fails" in the OpenStack documentation at
http://docs.openstack.org/admin-guide-cloud/content/section_network-troubleshoot.html

## Slow Performance, Watchdog Issues, and High CPU Usage on KVM Deployments

**Problem**

Appliance performance is slow, watchdog issues occur, and the appliance shows unusually high CPU usage when running on an Ubuntu virtual machine.

**Solution**

Install the latest Host OS updates from Ubuntu.

## General Troubleshooting for Virtual Appliances Running on Linux Hosts

**Problem**

Issues with virtual appliances running on KVM deployments may be related to host OS configuration issues.

**Solution**

See the troubleshooting section and other information in the *Virtualization Deployment and Administration Guide* available from:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/pdf/Virtualization_Deployment_and_Administration_Guide/Red_Hat_Enterprise_Linux-7-Virtualization_Deployment_and_Administration_Guide-en-US.pdf.

# WCCP Problems

• Maximum Port Entries, on page 581

## Maximum Port Entries

In deployments using WCCP, the maximum number of port entries is 30 for HTTP, HTTPS , and FTP ports combined.

# Packet Capture

• Starting a Packet Capture, on page 581
• Managing Packet Capture Files, on page 582

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.

Web Security Appliance  does not support packet capture for the NIC paired interfaces. The packet capture will be applied only for the active interface. For example, if both P1 and P2 are paired, both P1 and P2 will not be configured in the user interface or the CLI.

## Starting a Packet Capture

**Procedure**

**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. One 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:<br>• **Run Capture Until File Size Limit Reached**. The capture runs until the file limit set above is reached.<br>• **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.<br>• **Run Capture Indefinitely.** The packet capture runs until you manually stop it.<br>**Note**<br>The capture can be ended manually at any time. |
| 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:<br>• **No Filters.** All packets will be captured.<br>• **Predefined Filters.** The predefined filters provide filtering by port and/or IP addresses. If left blank, all traffic will be captured.<br>• **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, on page 582

## Downloading or Deleting Packet Capture Files

**Note** You can also connect to the appliance using FTP and retrieving packet capture files from the captures directory.

### Procedure

**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.

# Working With Support


- Gathering Information for Efficient Service , on page 583
- Opening a Technical Support Request, on page 583
- Getting Support for Virtual Appliances , on page 584
- Enabling Remote Access to the Appliance , on page 584


## Gathering Information for Efficient Service

Before contacting Support:

- Enable custom logging fields as described in General Troubleshooting Best Practices, on page 555.
- Consider doing a packet capture. See Packet Capture, on page 581.

## Opening a Technical Support Request

### 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.

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.

### Procedure

**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.

# Getting Support for Virtual Appliances

If you file a support case for a Cisco content security virtual appliance, you must provide your Virtual License Number (VLN), your contract number, and your Product Identifier code (PID).

You can identify your PID based on the software licenses running on your virtual appliance, by referencing your purchase order, or from the following table:

| Functionality | PID | Description |
|---|---|---|
| Web Security Essentials | WSA-WSE-LIC= | Includes:<br>• Web Usage Controls<br>• Web Reputation |
| Web Security Premium | WSA-WSP-LIC= | Includes:<br>• Web Usage Controls<br>• Web Reputation<br>• Sophos and Webroot Anti-Malware signatures |
| Web Security Anti-Malware | WSA-WSM-LIC= | Includes Sophos and Webroot Anti-Malware signatures |
| McAfee Anti-Malware | WSA-AMM-LIC= | — |
| Advanced Malware Protection | WSA-AMP-LIC= | — |

# Enabling Remote Access to the Appliance

The Remote Access option allows Cisco Customer Support to remotely access your appliance for support purposes.

**Procedure**

**Step 1** Choose **Support And Help > Remote Access**.

**Step 2** Click **Enable**.

**Step 3** Complete the Customer Support Remote Access options:

| Option | Description |
|---|---|
| Seed String | If you enter a string, the string should not match any existing or future pass phrase.<br>The string will appear near the top of the page after you click Submit.<br>You will give this string to your support representative. |
| Secure Tunnel (recommended) | Specifies whether or not to use a secure tunnel for remote access connections.<br>When enabled, the appliance creates an SSH tunnel over the specified port to the server upgrades.ironport.com, 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.<br>Once the techsupport tunnel is enabled, it will remain connected to upgrades.ironport.com 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.<br>The Remote Access account will remain active until specifically deactivated. |
| Appliance Serial Number | The serial number of the appliance. |

**Step 4** Submit and commit your changes.

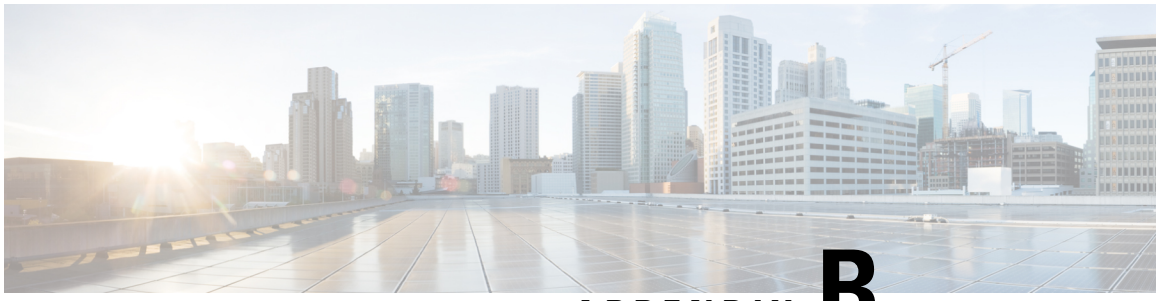
**Step 5** Look for the seed string in the Success message near the top of the page and make a note of it.

For security reasons, this string is not stored on the appliance and there is no way to locate this string later.

Keep this seed string in a safe place.

**Step 6** Give the seed string to your Support representative.

Troubleshooting



APPENDIX B

# Command Line Interface

This topic contains the following sections:


- Overview of the Command Line Interface , on page 587
- Accessing the Command Line Interface, on page 587
- General Purpose CLI Commands, on page 590
- Web Security Appliance  CLI Commands, on page 591


# 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 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.

## First Access

You can add other users with differing levels of permissions after you have accessed the CLI the first time using the **admin** account—log in to the appliance by entering the default **admin** user name and passphrase:

- User name: **admin**
- Passphrase: **ironport**

The System Setup Wizard prompts you to change the passphrase for the **admin** account the first time you log in with the default passphrase.

You can also reset the **admin** account passphrase at any time using the `passwd` command.

# Subsequent Access

You can connect and log into the appliance at any time, using a valid user name and passphrase. Note that a listing of recent appliance access attempts, both successes and failures, for the current user name is displayed automatically upon log-in.

See the following `userconfig` command description, or Administering User Accounts, on page 509 for information about configuring additional users.

# 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, pressing 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 (press the Tab key)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth (pressing the Tab again completes the entry with sethostname)
example.com> sethostname
```

## Committing Configuration Changes Using the CLI

- Many configuration changes do not take effect until you commit them.
- The `commit` command allows you to change configuration settings while other operations proceed normally.
- 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.
- 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.
- Changes are not actually committed until you receive confirmation and a timestamp.

# General Purpose CLI Commands

This section describes some basic commands you might use in a typical CLI session, such as committing and clearing changes.

## CLI Example: Committing Configuration Changes

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
```

## CLI Example: 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>
```

# CLI Example: 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
```

# CLI Example: 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
```

Further, you can access help for a specific command by entering **`help`** `commandname`.

### Related Topics

- Web Security Appliance CLI Commands, on page 591

# 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.

**Note** Not all CLI commands are applicable/available in all operating modes (Standard and Cloud Web Security Connector).

### adminaccessconfig

You can configure the Web Security Appliance  to have stricter access requirements for administrators logging into the appliance, and you can specify an inactivity time-out value. See Additional Security Settings for Accessing the Appliance, on page 515 and User Network Access, on page 516 for more information.

### advancedproxyconfig

Configure advanced Web Proxy options; subcommands are:

**`AUTHENTICATION`** – Authentication configuration options:

- `When would you like to forward authorization request headers to a parent proxy`
- `Enter the Proxy Authorization Realm to be displayed in the end user authentication dialog`
- `Would you like to log the username that appears in the request URI`

- Should the Group Membership attribute be used for directory lookups in the Web UI (when it is not used, empty groups and groups with different membership attributes will be displayed)
- Would you like to use advanced Active Directory connectivity checks
- Would you like to allow case insensitive username matching in policies
- Would you like to allow wild card matching with the character * for LDAP group names
- Enter the charset used by the clients for basic authentication [ISO-8859-1/UTF-8]
- Would you like to enable referrals for LDAP
- Would you like to enable secure authentication
- Enter the hostname to redirect clients for authentication
- Enter the surrogate timeout for user credentials
- Enter the surrogate timeout for machine credentials
- Enter the surrogate timeout in the case traffic permitted due to authentication service unavailability
- Enter re-auth on request denied option [disabled / embedlinkinblockpage]
- Would you like to send Negotiate header along with NTLM header for NTLMSSP authentication
- Configure username and IP address masking in logs and reports
- Timeout to enable/disable local Auth cache.

  You can use this CLI option to enable or disable the proxy process immediate authentication cache. The time set is in seconds. By default this option is enabled and set for 30 seconds. It must be shorter than IP surrogate time.

**CACHING** – Proxy Caching mode; choose one:

- Safe Mode
- Optimized Mode
- Aggressive Mode
- Customized Mode

See also Choosing The Web Proxy Cache Mode, on page 69.

**DNS** – DNS configuration options:

- Enter the URL format for the HTTP 307 redirection on DNS lookup failure
- Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure
- Would you like proxy not to automatically failover to DNS results when upstream proxy (peer) is unresponsive
- Do you want to disable IP address in Host Header
- Find web server by:

0 = Always use DNS answers in order

1 = Use client-supplied address then DNS

2 = Limited DNS usage

3 = Very limited DNS usage

The default value is 0. For options 1 and 2, DNS will be used if Web Reputation is enabled. For options 2 and 3, DNS will be used for explicit proxy requests, if there is no upstream proxy or in the event the configured upstream proxy fails. For all options, DNS will be used when Destination IP Addresses are used in policy membership.

**EUN** – End-user notification parameters:

- Choose:

  1. Refresh EUN pages

  2. Use Custom EUN pages

  3. Use Standard EUN pages

- Would you like to turn on presentation of the User Acknowledgement page?

See also Web Proxy Usage Agreement, on page 75 and End-User Notifications Overview, on page 327.

**NATIVEFTP** – Native FTP configuration:

- Would you like to enable FTP proxy
- Enter the ports that FTP proxy listens on
- Enter the range of port numbers for the proxy to listen on for passive FTP connections
- Enter the range of port numbers for the proxy to listen on for active FTP connections
- Enter the authentication format:

  1. Check Point

  2. No Proxy Authentication

  3. Raptor

- Would you like to enable caching
- Would you like to enable server IP spoofing
- Would you like to enable client IP spoofing
- Would you like to pass FTP server welcome message to the clients
- Enter the max path size for the ftp server directory

See alsoOverview of FTP Proxy Services, on page 80.

**FTPOVERHTTP** – FTP Over HTTP options:

- Enter the login name to be used for anonymous FTP access
- Enter the password to be used for anonymous FTP access

See also Overview of FTP Proxy Services, on page 80.

**Highperformance-** enable and disable the high performance mode.

**HTTPS** – HTTPS-related options:

- HTTPS URI Logging Style - fulluri or stripquery
- Would you like to decrypt unauthenticated transparent HTTPS requests for authentication purpose
- Would you like to decrypt HTTPS requests for End User Notification purpose
- Action to be taken when HTTPS servers ask for client certificate during handshake:

  1. Pass through the transaction
  2. Reply with certificate unavailable

- Do you want to enable server name indication (SNI) extension?
- Do you want to enable automatic discovery and download of missing Intermediate Certificates?
- Do you want to enable session resumption?

See also Overview of Create Decryption Policies to Control HTTPS Traffic, on page 241.

**SCANNING** – Scanning options:

- Would you like the proxy to do malware scanning all content regardless of content type
- Enter the time to wait for a response from an anti-malware scanning engine (Sophos, McAfee, or Webroot), in seconds
- Do you want to disable Webroot body scanning

See also Overview of Anti-Malware Scanning , on page 266 and Overview of Scanning Outbound Traffic, on page 257.

**SCANNERS-** You can use the scanners subcommand to configure the settings for scanner engines. To use the scanners subcommand, you must disable the 'Adaptive Scanning' feature.

- Choose the operation you want to perform:

  AMP - Secure Endpoint related option

  SOPHOS - Sophos Memory related option

- **AMP** – Using this command, you can add the MIME types that need not be scanned by the AMP engine to increase the scanning performance. Default MIME type options are 'image/ALL and text/ALL'.

  To add the MIME types, you must append them after the default options. For example, if you want to add the video and audio MIME types, the format must be:

  'image/ALL and text/ALL video/ALL audio/ALL'

- **SOPHOS** – Sophos engine scan may get timed out and run out of memory when there is a huge traffic running through the engine. This is due to malloc memory issue, you can use the sophos subcommand and then choose MALLOC_SETTING to resolve this issue. When you select MALLOC_SETTING, you will be prompted with following message:

```
Changing Sophos Malloc Settings will lead to stoppage of coredumps.
Do you want to change the sophos malloc settings ? [Y]>
```

If you select yes, malloc settings will be changed and sophos will get restarted. To revert to default settings, you can use the same command.

**Note** Before using the command, we recommend you to take a note of the following:

- Make sure no traffic is running while changing the sophos malloc settings.
- When you change the settings from the CLI, the changes may take some time to update since sophos requires a restart.
- Do not change the malloc settings frequently.

**Note** For TAC use only.

- If sophos is coring due to any windows/linux update traffic, you must only change the malloc settings after the coring is completed.
- After the sophos restart, you might see the coring once because the changes will take some time to update.

**PROXYCONN** – Manage the list of user agents that cannot accept the proxy connection header. The list entries are interpreted as regular expressions in Flex (Fast Lexical Analyzer) dialect. A user agent will be matched if any substring of it matches any regular expression in the list.

- Choose the operation you want to perform:

```
NEW - Add an entry to the list of user agents

DELETE - Remove an entry from the list
```

**CUSTOMHEADERS** – Manage custom request headers for specific domains.

- Choose the operation you want to perform:

```
DELETE - Delete entries

NEW - Add new entries

EDIT - Edit entries
```

See also Adding Custom Headers To Web Requests, on page 72.

**MISCELLANEOUS** – Miscellaneous proxy-related parameters:

- `Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)`
- `Would you like proxy to perform dynamic adjustment of TCP receive window size`
- `Would you like proxy to perform dynamic adjustment of TCP send window size`

- Do you want to filter non-HTTP responses?

  (Non-HTTP responses are filtered by default.Enter **N** if you want to allow non-HTTP responses via proxy)
- Enable caching of HTTPS responses
- Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds)
- Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)
- Mode of the proxy:

  1. Explicit forward mode only
  2. Transparent mode with L4 Switch or no device for redirection
  3. Transparent mode with WCCP v2 Router for redirection
- Spoofing of the client IP by the proxy:

  1. Enable for all requests
  2. Enable for transparent requests only
- Do you want to pass HTTP X-Forwarded-For headers?
- Do you want to enable server connection sharing?
- Would you like to permit tunneling of non-HTTP requests on HTTP ports?
- Would you like to block tunneling of non-SSL transactions on SSL Ports?
- Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses?
- Do you want proxy to throttle content served from cache?
- Would you like the proxy to use client IP addresses from X-Forwarded-For headers
- Do you want to forward TCP RST sent by server to client?
- Do you want to enable WCCP proxy health check?
- Do you want to enable URL lower case conversion for velocity regex?

See also Using the P2 Data Interface for Web Proxy Data , on page 38 and Configuring Web Proxy Settings, on page 65.

**socks** – SOCKS Proxy options:

- Would you like to enable SOCKS proxy
- Proxy Negotiation Timeout
- UDP Tunnel Timeout
- SOCKS Control Ports
- UDP Request Ports

See also Using the P2 Data Interface for Web Proxy Data , on page 38 and SOCKS Proxy Services, on page 82.

`CONTENT-ENCODING` – Allow and block content-encoding types.

Currently allowed content-encoding type(s): compress, deflate, gzip

Currently blocked content-encoding type(s): N/A

To change the setting for a specific content-encoding type, select an option:

1. compress

2. deflate

3. gzip

[1]>

The encoding type "compress" is currently allowed

Do you want to block it? [N]>



**Note** The **centralauthcache** command is applicable for high performance enabled devices and to improve authentication cache performance.

#### adminaccessconfig

You can configure the Web Security Appliance to have stricter access requirements for administrators logging into the appliance.

#### alertconfig

Specify alert recipients, and set parameters for sending system alerts.

#### authcache

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.



**Note** When *centralauthcache* is enabled, the *authcache* command does not display ISE authenticated user name. To obtain the ISE user information, use the *isedata* command.

#### bwcontrol

Enable bandwidth control debug messages in the Default Proxy log file.

- **bwcontrol startlog**—Enable logging of bandwidth control debug messages to proxy logs.
- **bwcontrol stoplog**—Disable logging of bandwidth control debug messages.

#### certconfig

`SETUP` – Configure security certificates and keys.

`OCSPVALIDATION` – Enable/disable OCSP validation of certificate during upload.

### clear

Clears pending configuration changes since last commit.

### commit

Commits pending changes to the system configuration.

### configbackup

Saves backup configuration file and sends the file to a remotely located backup server through FTP or SCP

### csidconfig

You can configure different parameters of the Cisco Success Network feature on the appliance related to the publishing of telemetry data to the security services exchange portal.

Subcommands are:

- `CISCO_SUCCESS_NETWORK` – To enable/disable sending your appliance details and feature usage to Cisco.
- `CSIDATAPUSHINTERVAL` – Configure time interval of telemetry data push.

### createcomputerobject

Creates a computer object at the location you specify.

### curl

Send a cURL request directly to a Web server, or to a Web server via proxy, with the request and response HTTP headers returned to let you determine why a Web page is failing to load.



**Note** This command is for Administrator or Operator use only, under TAC supervision.

Subcommands are:

- `DIRECT` – URL access going direct
- `APPLIANCE` – URL access through the Appliance

### datasecurityconfig

Defines a minimum request body size, below which upload requests are not scanned by the Cisco Data Security Filters.

### date

Displays the current date. Example:

```
Thu Jan 10 23:13:40 2013 GMT
```

### diagnostic

Proxy- and reporting-related subcommands:

**NET** – Network Diagnostic Utility

This command has been deprecated; use packetcapture to capture network traffic on the appliance.

**PROXY** – Proxy Debugging Utility

Choose the operation you want to perform:

- SNAP – Take a snapshot of the proxy
- OFFLINE – Take the proxy off-line (via WCCP)
- RESUME – Resume proxy traffic (via WCCP)
- CACHE – Clear proxy cache

**proxyscannermap-** This command displays PID mapping between each proxy and corresponding scanner process.

**REPORTING** – Reporting Utilities

The reporting system is currently enabled.

Choose the operation you want to perform:

- DELETEDB – Re-initialize the reporting database
- DISABLE – Disable the reporting system
- DBSTATS – List DB and Export Files (Displays the list of unprocessed files and folders under export_files and always_onbox folders.)
- DELETEEXPORTDB – Delete Export Files (Deletes all unprocessed files and folders under export_files and always_onbox folders.)
- DELETEJOURNAL – Delete Journal Files(Deletes all aclog_journal_files.)

### dnsflush

Flush DNS entries on the appliance.

### etherconfig

Configure Ethernet port connections.

Choose the operation you want to perform:

- MEDIA – View and edit ethernet media settings.
- PAIRING – View and configure NIC Pairing.
- VLAN – View and configure VLANs.
- MTU – View and configure MTU.

### externaldlpconfig

Defines a minimum request body size, below which upload requests are not scanned by the external DLP server.

### externaldlpconfig

Defines a minimum request body size, below which upload requests are not scanned by the external DLP server.

### featurekey

Submits valid keys to activate licensed features.

### featurekeyconfig

Automatically check for and update feature keys.

### `fipsconfig`

**`SETUP`** – Enable/disable FIPS 140-2 compliance, and encryption of Critical Sensitive Parameters (CSP). Note that an immediate reboot will be necessary.

**`FIPSCHECK`** – Check FIPS mode compliance. Indicates whether various certificates and services are FIPS compliant.

See FIPS Compliance, on page 529 for additional information.

### grep

Searches named input files for lines containing a match to the given pattern.

### gathererdconfig

Configure the polling functionality between the appliance and the authentication server.

### help

Returns a list of commands.

### httppatchconfig

Enables or disables outgoing HTTP PATCH requests. The default value is disable.

### 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.

### iseconfig

Displays current ISE configuration parameters; specify an ISE configuration operation to perform:

**Note** The `setup` command is updated to `ISE RECONCILIATION TIME SETUP` command for AsyncOS version 12.7 only.

**Note** The setup command is not applicable for Secure Web Appliance 12.7.

`ISE RECONCILIATION TIME SETUP`—Configure ISE reconciliation time setup. To restart the ised process automatically, set the time in the HH::MM format within 24 hours of ISE configuration. After a restart, the bulk download takes place.

```
Choose the operation you want to perform:
- Schedule ISE Restart Time in HH:MM format.
- Modify cache timeout for ISE users. Specify a timeout value in hours, upto 24 hours
```

By default, the value for option 1 is 00:00 mid-night.

### isedata

Specify an ISE data-related operation:

`statistics` – Show ISE server status and ISE statistics.

`cache` – Show the ISE cache, or check an IP address:

`sgts` – Show the ISE Secure Group Tag (SGT) table.

`groups` – Show the ISE Groups table.

If VDI is implemented, the sub commands `show` and `checkip` under the main command `cache` displays more details. The `show` subcommand displays details about port range and `checkip` subcommand displays details about the VDI user such as IP address, name, port range etc.

```
[]> cache

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
```

### 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.

### maxhttpheadersize

Set the maximum HTTP header size or URL size for proxy requests; enter the value in bytes, or append a K to the number to indicate kilobytes.

Policy Trace can fail for a user that belongs to a large number of authentication groups. It can also fail if the HTTP response header size or URL size is greater than the current “max header size.” Increasing this value can alleviate such failures. Minimum value is 32 KB; default value is 32 KB; maximum value is 1024 KB.

### modifyauthhelpers

Use this command to configure the number of Kerberos authentication helpers within a range of 5 to 21 for BASIC, NTLMSSP, and NEGO.

### 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:

- 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.

### networktuning

The Web Security Appliance utilizes several buffers and optimization algorithms to handle hundreds of TCP connections simultaneously, providing high performance for typical Web traffic—that is, short-lived HTTP connections.

In certain situations, such as frequent downloading of large files (100+ MB), larger buffers can provide better per-connection performance. However, overall memory usage will increase, and thus any buffer increases should be in line with the memory available on the system.

The send- and receive-space variables represent the buffers used for storing data for communications over any given TCP socket. The send- and receive-auto variables are used to enable and disable the FreeBSD auto-tuning algorithm for dynamically controlling window size. These two parameters are applied directly in the FreeBSD kernel.

When `SEND_AUTO` and `RECV_AUTO` are enabled, the system tunes the window size dynamically based on system load and available resources. On a lightly loaded Web Security Appliance , the system attempts to keep window sizes large to reduce per transaction latency. The maximum value of the dynamically tuned window size is dependent on the configured number of mbuf clusters, which in turn is dependent on the total RAM available on the system. As the total number of client connections increases, or when the available network buffer resources become scarce, the system tunes down the window sizes to protect itself from losing all network buffer resources to proxied traffic.

See Upload/Download Speed Issues, on page 561 for additional information about using this command.

The `networktuning` subcommands are:

**`SENDSPACE`** – TCP send-space buffer size; range is from 8192 to 131072 bytes; the default is 16000 bytes.

**`RECVSPACE`** – TCP receive-space buffer size; range is from 8192 to 131072 bytes; the default is 32768 bytes.

**`SEND-AUTO`** – Enable/disable TCP send auto-tuning; 1 = On, 0 = Off; default is Off. If you enable TCP send auto-tuning, be sure to use `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP send window size?` to disable send buffer auto-tuning.

**`RECV-AUTO`** – Enable/disable TCP receive auto-tuning; 1 = On, 0 = Off; default is Off. If you enable TCP receive auto-tuning, be sure to use `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP receive window size? Yes` to disable receive buffer auto-tuning.

**`MBUF CLUSTER COUNT`** – Change the number of available mbuf clusters; acceptable range is from 98304 to 1572864. The value should vary according to installed system memory, using this calculation: 98304 * (X/Y) where is X is gigabytes of RAM on the system and Y is 4 GB. For example, with 4 GB RAM, the recommended value is 98304 * (4/4) = 98304. Linear scaling is recommended as RAM increases.

**`SENDBUF-MAX`** – Specify the maximum send buffer size; range is from 131072 bytes to 2097152 bytes; the default is 1 MB.

**`RECVBUF-MAX`** – Specify the maximum receive buffer size; range is from 131072 bytes to 2097152 bytes; the default is 1 MB.

**`CLEAN-FIB-1`** – Remove all M1/M2 entries from the data-routing table—essentially, enable control-plane/data-plane separation. That is, disable any data-plane process from sending data over the M1 interface when “Separate Routing” is enabled. Data-plane processes are those for which “Use data routing table” is enabled, or which carry strictly non-management traffic. Control-plane processes can still send data of over either the M1 or P1 interfaces.

Following any changes to these parameters, be sure to commit your changes and the restart the appliance.



**Caution** Use this command only if you understand the ramifications. We recommend using only with TAC guidance.

### 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 passphrase.

### 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.

### quotaquery

To check or reset the volume and time used by a category.

Choose the operation you want to perform:

- `RESET`—Reset quota for specific entry in proxy quota cache.
- `SEARCH`—Search list of user entries in proxy quota cache.
- `RESETALL`—Reset all entries in proxy quota cache.



**Note** In a multi-proxy mode, when you want to reset the appliance while accessing *quotoquery* from the CLI, if the quota username consists of a "\" character, append another "\", and then reset the appliance. For example, if you find a quota username "vol:W2012-01\administrator@AD1", before performing a reset, edit the quota username (add additional "\") as "W2012-01\\administrator@AD1". The prefix "vol:" is not required when you perform a reset.

### 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.

### revert

Revert the AsyncOS for Web operating system to a previous qualified build. This is a very destructive action, destroying all configuration logs and databases. Refer to Reverting to a Previous Version of AsyncOS for Web, on page 546 for information about using this command.

### rollbackconfig

Allows you to rollback to one of the previously committed 10 configurations. By default, the rollback configuration feature is enabled.

### 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.

If FIPS mode is enable, provide a passphrase-handling option: `Mask passphrases` or `Encrypt passphrases`.

### 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”.

- `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 passphrases 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.

### smtpconfig

Configure the local host to listen for SNMP queries and allow SNMP requests.

### sshconfig

Configure hostname and host key options for trusted servers.

### sslconfig

The default cipher for AsyncOS versions 9.0 and earlier is `DEFAULT:+kEDH`.

The default cipher for AsyncOS versions 9.1 - 11.8 is:

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
!AES256-SHA:DHE-RSA-AES128-SHA
```

In this case, the default cipher may change based on your ECDHE cipher selections.

The default cipher for AsyncOS versions 12.0 and later is:

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```



**Note** Update the default cipher suite while upgrading to a newer AsyncOS version. The ciphers suites are not automatically updated. When you upgrade from an earlier version to AsyncOS 12.0 and later, Cisco recommends updating the cipher suite to:

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

**FALLBACK** – Enable/disable the SSL/TLS fall-back option. If enabled, communications with remote servers will fall back to the lowest configured protocol following a handshake failure.

After a protocol version is negotiated between client and server, handshake failure is possible because of implementation issues. If this option is enabled, the proxy attempts to connect using the lowest version of the currently configured TLS/SSL protocols.

**Note** On new AsyncOS 9.x installations, fall-back is disabled by default. For upgrades from earlier versions on which the fall-back option exists, the current setting is retained; otherwise, when upgrading from a version on which the option did not exist, fall-back is enabled by default.

**ECDHE** – Enable/disable use of ECDHE ciphers for LDAP.

Additional ECDH ciphers are supported in successive releases; however, certain named curves provided with some of the additional ciphers cause the appliance to close a connection during secure LDAP authentication and HTTPS traffic decryption. See SSL Configuration , on page 532for more information about specifying additional ciphers.

If you experience these issues, use this option to disable or enable ECDHE cipher use for either or both features.

### ssltool

Executes different OPENSSL commands from appliance's CLI to troubleshoot SSL connections. The `ssltool` command has the following subcommands:

- **sclient** -This is CLI version of openssl s_client command. It will connect to a remote host using SSL/TLS directly without using the appliance.
  - `COMMAND` - Executes an openssl s_client command. The following openssl s_client commands are supported:

    ```
    -connect, -servername, -verify, -cipher, -verify_return_error, -reconnect, -pause,
     -showcerts, -prexit, -state, -debug, -msg, -tls1, -tls1_1, -tls1_2, -no_ssl2,
    -no_ssl3, -no_tls1, -no_tls1_1, -no_tls1_2, -tlsextdebug, -no_ticket, -status,
    -save, -noout
    ```

    See the inline help for more information about the supported openssl s_client commands .

**Note** After you execute the `command`, you can save the output to a file using the `-save` option. You cannot access the saved log files. These log files are used by Cisco support team for debugging.

  - `HELP` - Provides help information.

- **CLEARLOGS** -Deletes all logs generated by `ssltool`.

### status

Displays system status.

### supportrequest

Send the support request email to Cisco Customer Support. This includes system information and a copy of the primary configuration.

(Optional) If you provide the service request number, a larger set of system and configuration information is added to the service request automatically. This information is zipped and uploaded to the service request using FTP.

### tail

Displays the end of a log file. Command accepts log file name as parameter.

Example 1

```
example.com> tail
Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
…
…
Enter the number of the log you wish to tail.
[]> 9
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 10:03:07 2017 Info: Begin Logfile
~
~
…
…
“CTRL-C” + “q”
```

Example 2

```
example.com> tail system_logs
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 09:59:10 2017 Info: Begin Logfile
…
…
“CTRL-C” + “q”
```

### tcpservices

Displays information about open TCP/IP services.

### techsupport

Provides a temporary connection to allow Cisco Customer Support to access the system and assist in troubleshooting.

### telnet

Communicates with another host using the TELNET protocol, usually used to check connectivity.

### testauthconfig

Tests the authentication settings for a given authentication realm against the authentication servers defined in the realm.

### testauthconfig [-d level] [realm name]

Running the command without any option causes the appliance to list the configured authentication realms from which you can make a selection.

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.



**Note** Cisco recommends you use level 0. Only use a different debug level when you need more detailed information to troubleshoot.

### tuiconfig tuistatus

These two commands are documented in Using the CLI to Configure Advanced Transparent User Identification Settings, on page 96.

### traceroute

Traces IP packets through gateways and along the path to a destination host.

### trailblazerconfig

You can use the `trailblazerconfig` command to route your incoming and outgoing connections through HTTP and HTTPS ports on the new web interface.



**Note** By default, `trailblazerconfig` CLI command is enabled on your appliance. You can see the inline help by typing the command: `help trailblazerconfig`.

The syntax is as follows:

```
trailblazerconfig enable <https_port> <http_port>

trailblazerconfig disable

trailblazerconfig status
```

Where:

`'enable'` runs the trailblazer on the default ports (HTTPS: 4431 or HTTP: 801).

`'disable'` terminates the trailblazer

`'status'` checks the status of the trailblazer.



**Note** If you have enabled `trailblazerconfig` command on the appliance, the request URL will contain the HTTP/HTTPS port number appended to the hostname.

You can try any one of the following steps to make the navigation in your browser seamless:

- Accept the certificate used by the web interface and use the following URL syntax: `https://hostname:<https_api_port> (for example, https://some.example.com:6443)` in a new browser window and accept the certificate. Here `<https_api_port>` is the AsyncOS API HTTPS port configured in **Network > IP Interfaces**. Also, ensure that the API ports (HTTP/HTTPS) are opened on the firewall.
- By default, `trailblazerconfig` CLI command is enabled on your appliance. Make sure that the HTTP/HTTPS ports are opened on the firewall. Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.

  If the `trailblazerconfig` CLI command is disabled, you can run the **trailblazerconfig** > **enable** command using the CLI to avoid the following issues:

  - Requiring to add multiple certificates for API ports in certain browsers.
  - Redirecting to the legacy web interface when you refresh the Spam quarantine, Safelist or Blocklist page.
  - Metrics bar on the Advanced Malware Protection report page does not contain any data.

### updateconfig

Configure update and upgrade settings.

### updatenow

Update all components.

### upgrade

Install the Async OS software upgrade.

`downloadinstall` – Download and immediately install an upgrade package.

`download` – Download and save upgrade package for installation later.

After you enter either of these commands, a list of upgrade packages applicable for this Web Security Appliance is displayed. Select the desired package by entering its entry number and then pressing Enter; download begins in the background. During download, additional subcommands are available: `downloadstatus` and `canceldownload`.

When download is complete, if you initially entered `downloadinstall`, installation begins immediately. If you entered `download`, two additional commands are available when download is complete: `install` and `delete`. Enter `install` to begin installing a previously downloaded package. Use `delete` to remove the previously downloaded package from the Web Security Appliance .

### userconfig

Configure system administrators.

### version

Displays general system information, installed versions of system software, and rule definitions.

### wccpstat

`all` - Displays details of all WCCP (Web Cache Communication Protocol) service groups.

`servicegroup` - Displays details of a specific WCCP service group.

### 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 users logged into the system, for both CLI and Web interface sessions.

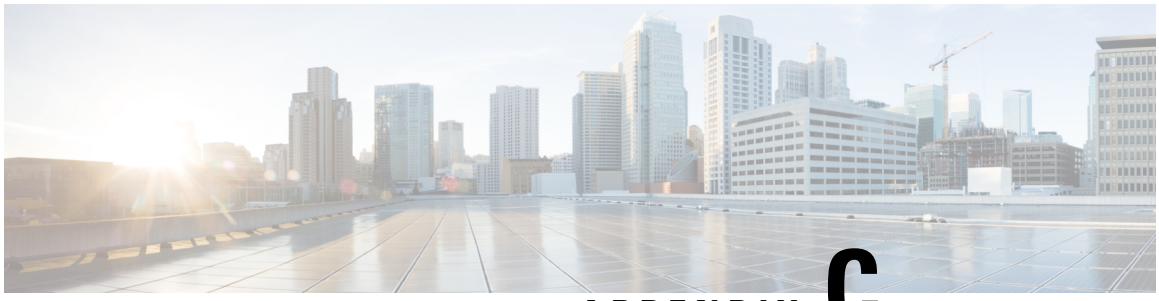


**Note** Individual users can have a maximum of 10 concurrent sessions.

### whoami

Displays user information.

Command Line Interface



APPENDIX C

# Additional Information

This topic contains the following sections:


- Cisco Notification Service , on page 613
- Documentation Set, on page 613
- Training, on page 614
- Knowledge Base Articles (TechNotes) , on page 614
- Cisco Support Community, on page 614
- Customer Support , on page 614
- Registering for a Cisco Account to Access Resources , on page 615
- Cisco Welcomes Your Comments, on page 615
- Third Party Contributors, on page 615
- Handling Personally Identifiable Information, on page 615


## Cisco Notification Service

Sign up to receive notifications relevant to your Cisco Content Security Appliances, such as Security Advisories, Field Notices, End of Sale and End of Support statements, and information about software updates and known issues.

You can specify options such as notification frequency and types of information to receive. You should sign up separately for notifications for each product that you use.

To sign up, visit http://www.cisco.com/cisco/support/notifications.html

A Cisco.com account is required. If you do not have one, see Registering for a Cisco Account to Access Resources , on page 615.

## Documentation Set

Related documentation for Cisco Web Security Appliance s is available from the following locations:

| Product | Link |
|---|---|
| Web Security Appliance s<br>(Includes hardware documentation.) | http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html |

| Product | Link |
|---|---|
| Content Security Management appliances<br>(Includes hardware documentation.) | http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html |
| Cisco Cloud Web Security<br>(Includes hardware documentation.) | http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html |

# Training

Training for Cisco email and web security products:

http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html

# Knowledge Base Articles (TechNotes)

### Procedure

**Step 1** Go to the main product page ( http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html).

**Step 2** Look for links with **TechNotes** in the name.

# Cisco Support Community

Access the Cisco Support Community for web security and associated management at the following URL:

https://supportforums.cisco.com/community/5786/web-security

The Cisco Support Community is a place to discuss general web security issues as well as technical information about specific Cisco products. For example, posts may include troubleshooting videos.

# Customer Support

Cisco TAC: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support site for legacy IronPort: http://www.cisco.com/web/services/acquisitions/ironport.html

For instructions for virtual appliances, see the *Cisco Content Security Virtual Appliance Installation Guide.*

For non-critical issues, you can also open a support case from the appliance.

### Related Topics

- Working With Support , on page 583

# 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

# 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.

# 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.

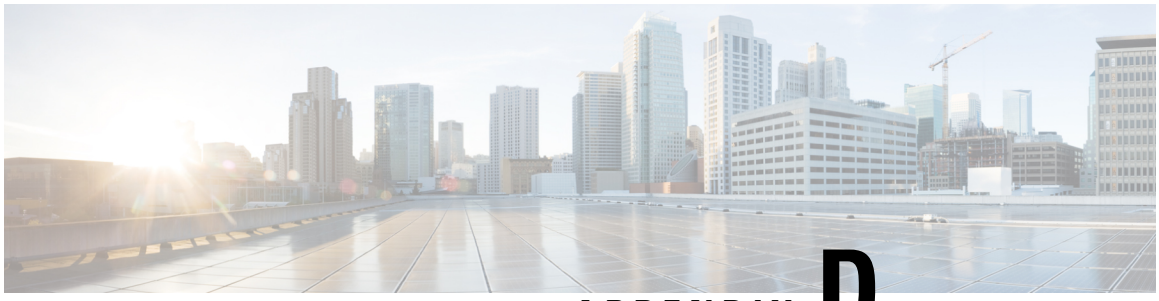
# Handling Personally Identifiable Information

To improve user experience, and send timely notifications and reports to you, Cisco Web Security Appliance collects your full name and email address.

The appliance collects this information when the administrator creates user accounts to manage Cisco Web Security Appliance . It is accessible only to the account owner and the administrator. Only the administrator can modify this information.

The information is stored locally within the appliance and not shared with any functions, teams, or third-party applications.

It is retained until the user has an active Cisco Web Security Appliance  account and is removed from the system when the administrator deletes the user account.



APPENDIX D

# End User License Agreement

This appendix contains the following sections:


- Cisco Systems End User License Agreement , on page 617
- Supplemental End User License Agreement for Cisco Systems Content Security Software , on page 623


# 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:

https://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 https://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 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 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 Web Security Appliance 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 https://www.cisco.com/c/en/us/about/legal/service-descriptions.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 Appliance , 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 https://www.cisco.com/c/en/us/about/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.