



## **AsyncOS 9.2 for Cisco Web Security Appliances User Guide**

Published: January 27, 2016

Revised: August 26, 2017

**Cisco Systems, Inc.**

[www.cisco.com](http://www.cisco.com)

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

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.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)).

This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

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

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

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

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

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

*AsyncOS 9.2 for Cisco Web Security Appliances User Guide*

© 2017 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### **Introduction to the Product and the Release 1-1**

    Introduction to the Web Security Appliance 1-1

    What's New 1-1

        What's New in Cisco AsyncOS 9.2 1-1

            What's New in Cisco AsyncOS 9.2.0-809 (GD) 1-1

            What's New in Cisco AsyncOS 9.2.0-796 1-2

            What's New in Cisco AsyncOS 9.2.0-083 (GD) 1-2

            What's New in Cisco AsyncOS 9.2.0-075 1-2

        Related Topics 1-2

    Using the Appliance Web Interface 1-2

        Web Interface Browser Requirements 1-2

        Enabling Access to the Web Interface on Virtual Appliances 1-3

        Accessing the Appliance Web Interface 1-3

        Committing Changes in the Web Interface 1-4

        Clearing Changes in the Web Interface 1-4

    The Cisco SensorBase Network 1-4

        SensorBase Benefits and Privacy 1-4

        Enabling Participation in The Cisco SensorBase Network 1-5

---

### CHAPTER 2

#### **Hybrid Web Security Mode 2-1**

    Overview of Hybrid Web Security Mode 2-1

    About Policy Application from Cloud Web Security 2-1

    WSA Functionality Not Available in Hybrid Mode 2-2

    Pre-configuration Requirements 2-2

    What To Do Next 2-3

---

### CHAPTER 3

#### **Connect, Install, and Configure 3-1**

    Overview of Connect, Install, and Configure 3-1

    Deploying a Virtual Appliance 3-2

        Migrating from a Physical to a Virtual Appliance 3-2

    Comparison of Modes of Operation 3-2

    Task Overview for Connecting, Installing, and Configuring 3-6

Connecting the Appliance	3-6
Gathering Setup Information	3-8
Registration with Cisco Cloud Web Security	3-9
Changing Registration on the Web Security appliance	3-9
System Setup Wizard	3-10
System Setup Wizard Reference Information	3-12
Network / System Settings	3-13
Network / Cloud Connector Settings	3-14
Network / Network Interfaces and Wiring	3-14
Network / Routes for Management and Data Traffic	3-15
Network / Transparent Connection Settings	3-15
Network /Administrative Settings	3-16
Security / Security Settings	3-16
Security / Upgrade Timing	3-17
Upstream Proxies	3-17
Upstream Proxies Task Overview	3-17
Creating Proxy Groups for Upstream Proxies	3-17
Network Interfaces	3-19
IP Address Versions	3-19
Enabling or Changing Network Interfaces	3-19
Configuring Failover Groups for High Availability	3-21
Add Failover Group	3-21
Edit High Availability Global Settings	3-22
View Status of Failover Groups	3-22
Using the P2 Data Interface for Web Proxy Data	3-22
Configuring TCP/IP Traffic Routes	3-23
Modifying the Default Route	3-24
Adding a Route	3-25
Saving and Loading Routing Tables	3-25
Deleting a Route	3-25
Configuring Transparent Redirection	3-25
Specifying a Transparent Redirection Device	3-25
Configuring WCCP Services	3-26
Increasing Interface Capacity Using VLANs	3-29
Configuring and Managing VLANs	3-29
Redirect Hostname and System Hostname	3-31
Changing the Redirect Hostname	3-32
Changing the System Hostname	3-32
Configuring SMTP Relay Host Settings	3-32

**CHAPTER 4**

Configuring an SMTP Relay Host	<b>3-33</b>
DNS Settings	<b>3-33</b>
Split DNS	<b>3-33</b>
Clearing the DNS Cache	<b>3-33</b>
Editing DNS Settings	<b>3-34</b>
Troubleshooting Connect, Install, and Configure	<b>3-35</b>

**Intercepting Web Requests** **4-1**

Overview of Intercepting Web Requests	<b>4-1</b>
Tasks for Intercepting Web Requests	<b>4-2</b>
Best Practices for Intercepting Web Requests	<b>4-2</b>
Web Proxy Options for Intercepting Web Requests	<b>4-3</b>
Configuring Web Proxy Settings	<b>4-3</b>
Web Proxy Cache	<b>4-5</b>
Clearing the Web Proxy Cache	<b>4-5</b>
Removing URLs from the Web Proxy Cache	<b>4-5</b>
Specifying Domains or URLs that the Web Proxy never Caches	<b>4-5</b>
Choosing The Web Proxy Cache Mode	<b>4-6</b>
Web Proxy Custom Headers	<b>4-8</b>
Adding Custom Headers To Web Requests	<b>4-8</b>
Web Proxy Bypassing	<b>4-9</b>
Web Proxy Bypassing for Web Requests	<b>4-9</b>
Configuring Web Proxy Bypassing for Web Requests	<b>4-9</b>
Configuring Web Proxy Bypassing for Applications	<b>4-9</b>
Web Proxy Usage Agreement	<b>4-10</b>
Client Options for Redirecting Web Requests	<b>4-10</b>
Troubleshooting Intercepting Requests	<b>4-10</b>

**CHAPTER 5****Acquire End-User Credentials** **5-1**

Overview of Acquire End-User Credentials	<b>5-1</b>
Authentication Task Overview	<b>5-2</b>
Authentication Best Practices	<b>5-2</b>
Authentication Planning	<b>5-2</b>
Active Directory/Kerberos	<b>5-3</b>
Active Directory/Basic	<b>5-4</b>
Active Directory/NTLMSSP	<b>5-5</b>
LDAP/Basic	<b>5-5</b>
Identifying Users Transparently	<b>5-5</b>

Understanding Transparent User Identification	5-6
Rules and Guidelines for Transparent User Identification	5-8
Configuring Transparent User Identification	5-9
Using the CLI to Configure Advanced Transparent User Identification Settings	5-9
Configuring Single-Sign-on	5-10
Authentication Realms	5-10
External Authentication	5-11
Configuring External Authentication through an LDAP Server	5-11
Enabling RADIUS External Authentication	5-11
Creating an Active Directory Realm for Kerberos Authentication Scheme	5-11
How to Create an Active Directory Authentication Realm (NTLMSSP and Basic)	5-14
Prerequisites for Creating an Active Directory Authentication Realm (NTLMSSP and Basic)	5-14
About Using Multiple NTLM Realms and Domains	5-14
Creating an Active Directory Authentication Realm (NTLMSSP and Basic)	5-15
Creating an LDAP Authentication Realm	5-16
About Deleting Authentication Realms	5-21
Configuring Global Authentication Settings	5-21
Authentication Sequences	5-26
About Authentication Sequences	5-27
Creating Authentication Sequences	5-27
Editing And Reordering Authentication Sequences	5-28
Deleting Authentication Sequences	5-28
Failed Authentication	5-28
About Failed Authentication	5-29
Bypassing Authentication with Problematic User Agents	5-29
Bypassing Authentication	5-31
Permitting Unauthenticated Traffic While Authentication Service is Unavailable	5-31
Granting Guest Access After Failed Authentication	5-31
Define an Identification Profile that Supports Guest Access	5-32
Use an Identification Profile that Supports Guest Access in a Policy	5-32
Configure How Guest User Details are Logged	5-32
Failed Authorization: Allowing Re-Authentication with Different Credentials	5-33
About Allowing Re-Authentication with Different Credentials	5-33
Allowing Re-Authentication with Different Credentials	5-33
Tracking Identified Users	5-33
Supported Authentication Surrogates for Explicit Requests	5-34
Supported Authentication Surrogates for Transparent Requests	5-34
Tracking Re-Authenticated Users	5-34
Credentials	5-35

Tracking Credentials for Reuse During a Session	<b>5-35</b>
Authentication and Authorization Failures	<b>5-36</b>
Credential Format	<b>5-36</b>
Credential Encryption for Basic Authentication	<b>5-36</b>
About Credential Encryption for Basic Authentication	<b>5-36</b>
Configuring Credential Encryption	<b>5-36</b>
Troubleshooting Authentication	<b>5-37</b>

---

**CHAPTER 6****Classify End-Users and Client Software** **6-1**

Overview of Classify Users and Client Software	<b>6-1</b>
Classify Users and Client Software: Best Practices	<b>6-2</b>
Identification Profile Criteria	<b>6-2</b>
Classifying Users and Client Software	<b>6-3</b>
Enable/Disable an Identity	<b>6-6</b>
Identification Profiles and Authentication	<b>6-7</b>
Troubleshooting Identification Profiles	<b>6-8</b>

---

**CHAPTER 7****Create Decryption Policies to Control HTTPS Traffic** **7-1**

Overview of Create Decryption Policies to Control HTTPS Traffic	<b>7-1</b>
Managing HTTPS Traffic through Decryption Policies Task Overview	<b>7-2</b>
Managing HTTPS Traffic through Decryption Policies Best Practices	<b>7-2</b>
Decryption Policies	<b>7-2</b>
Enabling the HTTPS Proxy	<b>7-3</b>
Controlling HTTPS Traffic	<b>7-5</b>
Configuring Decryption Options	<b>7-7</b>
Authentication and HTTPS Connections	<b>7-7</b>
Root Certificates	<b>7-7</b>
Managing Certificate Validation and Decryption for HTTPS	<b>7-8</b>
Valid Certificates	<b>7-8</b>
Invalid Certificate Handling	<b>7-9</b>
Uploading a Root Certificate and Key	<b>7-9</b>
Generating a Certificate and Key for the HTTPS Proxy	<b>7-10</b>
Configuring Invalid Certificate Handling	<b>7-10</b>
Options for Certificate Revocation Status Checking	<b>7-11</b>
Enabling Real-Time Revocation Status Checking	<b>7-12</b>
Trusted Root Certificates	<b>7-12</b>
Adding Certificates to the Trusted List	<b>7-13</b>
Removing Certificates from the Trusted List	<b>7-13</b>

Routing HTTPS Traffic	7-13
Troubleshooting Decryption/HTTPS/Certificates	7-14

---

**CHAPTER 8****Configuring Security Services** **8-1**

Overview of Web Reputation Filters	8-1
Web Reputation Scores	8-1
Understanding How Web Reputation Filtering Works	8-2
Web Reputation in Access Policies	8-2
Web Reputation in Cisco IronPort Data Security Policies	8-3
Overview of Anti-Malware Scanning	8-3
Understanding How the DVS Engine Works	8-3
Working with Multiple Malware Verdicts	8-3
Webroot Scanning	8-4
McAfee Scanning	8-4
Matching Virus Signature Patterns	8-5
Heuristic Analysis	8-5
McAfee Categories	8-5
Sophos Scanning	8-5
Understanding Adaptive Scanning	8-5
Adaptive Scanning and Access Policies	8-6
Maintaining the Database Tables	8-6
The Web Reputation Database	8-6
Logging of Web Reputation Filtering Activity and DVS Scanning	8-6
Logging Adaptive Scanning	8-7
Caching	8-7
Malware Category Descriptions	8-7

---

**CHAPTER 9****Notify End-Users of Proxy Actions** **9-1**

End-User Notifications Overview	9-1
Configuring General Settings for Notification Pages	9-2
End-User Acknowledgment Page	9-2
Access HTTPS and FTP Sites with the End-User Acknowledgment Page	9-3
About the End-user Acknowledgment Page	9-3
Configuring the End-User Acknowledgment Page	9-3
End-User Notification Pages	9-5
Configuring On-Box End-User Notification Pages	9-6
Off-Box End-User Notification Pages	9-7
Displaying the Correct Off-Box Page Based on the Reason for Blocking Access	9-7

URL Criteria for Off-Box Notification Pages	<b>9-7</b>
Off-Box End-User Notification Page Parameters	<b>9-7</b>
Redirecting End-User Notification Pages to a Custom URL (Off-Box)	<b>9-8</b>
Configuring the End-User URL Filtering Warning Page	<b>9-9</b>
Configuring FTP Notification Messages	<b>9-9</b>
Custom Messages on Notification Pages	<b>9-10</b>
Supported HTML Tags in Custom Messages on Notification Pages	<b>9-10</b>
Caveats for URLs and Logos in Notification Pages	<b>9-11</b>
Editing Notification Page HTML Files Directly	<b>9-12</b>
Requirements for Editing Notification HTML Files Directly	<b>9-12</b>
Editing Notification HTML Files Directly	<b>9-12</b>
Using Variables in Notification HTML Files	<b>9-13</b>
Variables for Customizing Notification HTML Files	<b>9-13</b>
Notification Page Types	<b>9-15</b>

---

**CHAPTER 10****Web Security Appliance Reports** **10-1**

Overview Page	<b>10-1</b>
System Capacity Page	<b>10-1</b>
System Status Page	<b>10-2</b>

---

**CHAPTER 11****Monitor System Activity Through Logs** **11-1**

Overview of Logging	<b>11-1</b>
Common Tasks for Logging	<b>11-2</b>
Best Practices for Logging	<b>11-2</b>
Troubleshooting Web Proxy Issues Using Logs	<b>11-2</b>
Log File Types	<b>11-3</b>
Adding and Editing Log Subscriptions	<b>11-7</b>
Pushing Log Files to Another Server	<b>11-11</b>
Archiving Log Files	<b>11-11</b>
Log File Names and Appliance Directory Structure	<b>11-12</b>
Reading and Interpreting Log Files	<b>11-12</b>
Viewing Log Files	<b>11-13</b>
Web Proxy Information in Access Log Files	<b>11-13</b>
Transaction Result Codes	<b>11-16</b>
ACL Decision Tags	<b>11-16</b>
Interpreting Access Log Scanning Verdict Entries	<b>11-20</b>
W3C Compliant Access Log Files	<b>11-24</b>

W3C Field Types	11-24
Interpreting W3C Access Logs	11-24
W3C Log File Headers	11-25
W3C Field Prefixes	11-25
Customizing Access Logs	11-26
Access Log User Defined Fields	11-26
Customizing Regular Access Logs	11-27
Customizing W3C Access Logs	11-27
Configuring CTA-specific Custom W3C Logs	11-28
Traffic Monitor Log Files	11-29
Interpreting Traffic Monitor Logs	11-29
Log File Fields and Tags	11-30
Access Log Format Specifiers and W3C Log File Fields	11-30
Malware Scanning Verdict Values	11-40
Troubleshooting Logging	11-41

---

CHAPTER 12

<b>Perform System Administration Tasks</b>	<b>12-1</b>
Overview of System Administration	12-1
Saving, Loading, and Resetting the Appliance Configuration	12-2
Viewing and Printing the Appliance Configuration	12-2
Saving the Appliance Configuration File	12-2
Loading the Appliance Configuration File	12-3
Resetting the Appliance Configuration to Factory Defaults	12-3
Working with Feature Keys	12-3
Displaying and Updating Feature Keys	12-4
Changing Feature Key Update Settings	12-4
Virtual Appliance License	12-4
Installing a Virtual Appliance License	12-5
Enabling Remote Power Cycling	12-5
Administering User Accounts	12-6
Managing Local User Accounts	12-6
Adding Local User Accounts	12-7
Deleting User Accounts	12-8
Editing User Accounts	12-8
Changing Passphrases	12-8
RADIUS User Authentication	12-8
Sequence of Events For Radius Authentication	12-8
Enabling External Authentication Using RADIUS	12-9

Defining User Preferences	<b>12-10</b>
Configuring Administrator Settings	<b>12-11</b>
Setting Passphrase Requirements for Administrative Users	<b>12-11</b>
Additional Security Settings for Accessing the Appliance	<b>12-12</b>
Resetting the Administrator Passphrase	<b>12-13</b>
Managing Alerts	<b>12-14</b>
Alert Classifications and Severities	<b>12-14</b>
Managing Alert Recipients	<b>12-14</b>
Adding and Editing Alert Recipients	<b>12-14</b>
Deleting Alert Recipients	<b>12-15</b>
Configuring Alert Settings	<b>12-15</b>
Alert Listing	<b>12-16</b>
Feature Key Alerts	<b>12-16</b>
Hardware Alerts	<b>12-17</b>
Logging Alerts	<b>12-17</b>
Reporting Alerts	<b>12-18</b>
System Alerts	<b>12-20</b>
Updater Alerts	<b>12-21</b>
Anti-Malware Alerts	<b>12-21</b>
System Date and Time Management	<b>12-21</b>
Setting the Time Zone	<b>12-22</b>
Synchronizing the System Clock with an NTP Server	<b>12-22</b>
SSL Configuration	<b>12-22</b>
Certificate Management	<b>12-24</b>
About Certificates and Keys	<b>12-24</b>
Managing Trusted Root Certificates	<b>12-24</b>
Certificate Updates	<b>12-25</b>
Viewing Blocked Certificates	<b>12-25</b>
Uploading or Generating a Certificate and Key	<b>12-25</b>
Uploading a Certificate and Key	<b>12-25</b>
Generating a Certificate and Key	<b>12-26</b>
Certificate Signing Requests	<b>12-26</b>
Intermediate Certificates	<b>12-27</b>
AsyncOS for Web Upgrades and Updates	<b>12-27</b>
Monitoring System Health and Status Using SNMP	<b>12-28</b>
MIB Files	<b>12-28</b>
Enabling and Configuring SNMP Monitoring	<b>12-28</b>
Hardware Objects	<b>12-29</b>
SNMP Traps	<b>12-29</b>

About the connectivityFailure SNMP Trap	12-29
CLI Example: snmpconfig	12-29

---

**APPENDIX A****Troubleshooting** **A-1**

General Troubleshooting Best Practices	<b>A-1</b>
Hybrid Web Security Issues	<b>A-2</b>
Registration (including Enrollment)	<b>A-2</b>
Policy Download	<b>A-2</b>
Policy Conversion	<b>A-2</b>
Hybrid Upgrade	<b>A-2</b>
Browser Problems	<b>A-2</b>
WPAD Not Working With Firefox	<b>A-3</b>
DNS Problems	<b>A-3</b>
Alert: Failed to Bootstrap the DNS Cache	<b>A-3</b>
Feature Keys Expired	<b>A-3</b>
Failover Problems	<b>A-3</b>
Failover Misconfiguration	<b>A-3</b>
Failover Issues on Virtual Appliances	<b>A-4</b>
FTP Problems	<b>A-4</b>
URL Categories Do Not Block Some FTP Sites	<b>A-4</b>
Large FTP Transfers Disconnect	<b>A-4</b>
Zero Byte File Appears On FTP Servers After File Upload	<b>A-5</b>
Chrome Browser Not Detected As User Agent in FTP-over-HTTP Requests	<b>A-5</b>
Hardware Issues	<b>A-5</b>
Cycling Appliance Power	<b>A-5</b>
Appliance Health and Status Indicators	<b>A-5</b>
Alert: Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware	<b>A-5</b>
HTTPS/Decryption/Certificate Problems	<b>A-6</b>
Accessing HTTPS Sites Using Routing Policies with URL Category Criteria	<b>A-6</b>
HTTPS Request Failures	<b>A-6</b>
HTTPS with IP-based Surrogates and Transparent Requests	<b>A-6</b>
Different Client “Hello” Behavior for Custom and Default Categories	<b>A-6</b>
Bypassing Decryption for Particular Websites	<b>A-7</b>
Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content	<b>A-7</b>
Alert: Problem with Security Certificate	<b>A-8</b>
Logging Problems	<b>A-8</b>
Custom URL Categories Not Appearing in Access Log Entries	<b>A-8</b>
Logging HTTPS Transactions	<b>A-8</b>

Alert: Unable to Maintain the Rate of Data Being Generated	A-9
Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs	A-9
Policy Problems	A-9
Blocked Object Problems	A-9
Some Microsoft Office Files Not Blocked	A-9
Blocking DOS Executable Object Types Blocks Updates for Windows OneCare	A-10
Identification Profile Disappeared from Policy	A-10
Policy Match Failures	A-10
Policy is Never Applied	A-10
HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication	A-10
User Matches Global Policy for HTTPS and FTP over HTTP Requests	A-11
User Assigned Incorrect Access Policy	A-11
Reboot Issues	A-11
Virtual Appliance Running on KVM Hangs on Reboot	A-11
Hardware Appliances: Remotely Resetting Appliance Power	A-12
Site Access Problems	A-12
Cannot Access URLs that Do Not Support Authentication	A-13
Cannot Access Sites With POST Requests	A-13
Upstream Proxy Problems	A-14
Upstream Proxy Does Not Receive Basic Credentials	A-14
Client Requests Fail Upstream Proxy	A-14
Unable to Route FTP Requests Via an Upstream Proxy	A-14
Virtual Appliances	A-14
Do Not Use Force Reset, Power Off, or Reset Options During AsyncOS Startup	A-14
Network Connectivity on KVM Deployments Works Initially, Then Fails	A-15
Slow Performance, Watchdog Issues, and High CPU Usage on KVM Deployments	A-15
General Troubleshooting for Virtual Appliances Running on Linux Hosts	A-15
WCCP Problems	A-15
Maximum Port Entries	A-15
Packet Capture	A-15
Starting a Packet Capture	A-16
Managing Packet Capture Files	A-16
Downloading or Deleting Packet Capture Files	A-17
Working With Support	A-17
Gathering Information for Efficient Service	A-17
Opening a Technical Support Request	A-17
Getting Support for Virtual Appliances	A-18
Enabling Remote Access to the Appliance	A-18

---

**APPENDIX B****Command Line Interface B-1**

Overview of the Command Line Interface	<b>B-1</b>
Accessing the Command Line Interface	<b>B-1</b>
First Access	<b>B-1</b>
Subsequent Access	<b>B-2</b>
Working with the Command Prompt	<b>B-2</b>
Command Syntax	<b>B-2</b>
Select Lists	<b>B-3</b>
Yes/No Queries	<b>B-3</b>
Subcommands	<b>B-3</b>
Escaping Subcommands	<b>B-4</b>
Command History	<b>B-4</b>
Completing Commands	<b>B-4</b>
Committing Configuration Changes Using the CLI	<b>B-4</b>
General Purpose CLI Commands	<b>B-4</b>
CLI Example: Committing Configuration Changes	<b>B-5</b>
CLI Example: Clearing Configuration Changes	<b>B-5</b>
CLI Example: Exiting the Command Line Interface Session	<b>B-5</b>
CLI Example: Seeking Help on the Command Line Interface	<b>B-5</b>
Web Security Appliance CLI Commands	<b>B-6</b>

---

**APPENDIX C****Additional Resources C-1**

Cisco Notification Service	<b>C-1</b>
Documentation Set	<b>C-2</b>
Training	<b>C-2</b>
Knowledge Base Articles (TechNotes)	<b>C-2</b>
Cisco Support Community	<b>C-2</b>
Customer Support	<b>C-2</b>
Registering for a Cisco Account to Access Resources	<b>C-3</b>
Third Party Contributors	<b>C-3</b>
Cisco Welcomes Your Comments	<b>C-3</b>

---

**APPENDIX D****End User License Agreement D-1**

Cisco Systems End User License Agreement	<b>D-1</b>
Supplemental End User License Agreement for Cisco Systems Content Security Software	<b>D-8</b>



# Introduction to the Product and the Release

---

- [Introduction to the Web Security Appliance, page 1-1](#)
- [What's New, page 1-1](#)
- [Using the Appliance Web Interface, page 1-2](#)
- [The Cisco SensorBase Network, page 1-4](#)

## Introduction to the Web Security Appliance

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

## What's New

- [What's New in Cisco AsyncOS 9.2, page 1-1](#)

## What's New in Cisco AsyncOS 9.2



**Note** This release is intended primarily for installing Hybrid Web Security on a device that has never been configured. Do not install or upgrade to this version unless you plan to operate the appliance in Hybrid mode.

- [What's New in Cisco AsyncOS 9.2.0-809 \(GD\), page 1-1](#)
- [What's New in Cisco AsyncOS 9.2.0-796, page 1-2](#)
- [What's New in Cisco AsyncOS 9.2.0-083 \(GD\), page 1-2](#)
- [What's New in Cisco AsyncOS 9.2.0-075, page 1-2](#)

### What's New in Cisco AsyncOS 9.2.0-809 (GD)

This is an upgrade release; no new features were added.

## What's New in Cisco AsyncOS 9.2.0-796

- Translation of both default and user-defined CWS policies to WSA policies has been expanded and optimized; very few CWS rules are not converted.
- Upgrades to the AsyncOS software are now downloaded automatically whenever available. Downloaded upgrades are then installed during the Time Windows specified on the Upgrade and Update Settings page.

## What's New in Cisco AsyncOS 9.2.0-083 (GD)

This is an upgrade release; no new features were added.

## What's New in Cisco AsyncOS 9.2.0-075

Hybrid Web Security mode provides unified cloud and on-premise policy enforcement and threat defense, using policies defined in Cisco ScanCenter—the administrative portal to Cloud Web Security—which are automatically downloaded to the Web Security appliance.

- [Related Topics, page 1-2](#)

## Related Topics

- Product release notes:  
[http://www.cisco.com/en/US/partner/products/ps10164/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/partner/products/ps10164/prod_release_notes_list.html)

# Using the Appliance Web Interface

- [Web Interface Browser Requirements, page 1-2](#)
- [Enabling Access to the Web Interface on Virtual Appliances, page 1-3](#)
- [Accessing the Appliance Web Interface, page 1-3](#)
- [Committing Changes in the Web Interface, page 1-4](#)
- [Clearing Changes in the Web Interface, page 1-4](#)

## Web Interface Browser Requirements

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

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

Your session automatically times out after 30 minutes of inactivity.

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

**Note**

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

## 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.

---

**Step 1** Access the command-line interface. See [Accessing the Command Line Interface, page B-1](#).

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

Pressing Enter at a prompt accepts the default value.

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

---

## Accessing the Appliance Web Interface

### Before You Begin

If you are using a virtual appliance, see [Enabling Access to the Web Interface on Virtual Appliances, page 1-3](#).

---

**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** 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 3** 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



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

---

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

## Clearing Changes in the Web Interface

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

## The Cisco SensorBase Network

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

## SensorBase Benefits and Privacy

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

Cisco recognizes the importance of maintaining your privacy, and does not collect or use personal or confidential information such as usernames and 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.

**Step 1** Choose to the **Security Services > SensorBase**.

**Step 2** Verify that SensorBase Network Participation is enabled.

When it is disabled, none of the data that the appliance collects is sent back to the SensorBase Network servers.

**Step 3** In the Participation Level section, choose one of the following levels:

- **Limited.** Basic participation summarizes server name information and sends MD5-hashed path segments to the SensorBase Network servers.
- **Standard.** Enhanced participation sends the entire URL with unobfuscated path segments to the SensorBase Network servers. This option assists in providing a more robust database, and continually improves the integrity of Web Reputation Scores.

**Step 4** In the AnyConnect Network Participation field, choose whether or not to include information collected from clients that connect to the Web Security appliance using Cisco AnyConnect Client.

AnyConnect Clients send their web traffic to the appliance using the Secure Mobility feature.

**Step 5** In the Excluded Domains and IP Addresses field, optionally enter any domains or IP addresses to exclude from traffic sent to the SensorBase servers.

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





## Hybrid Web Security Mode

- [Overview of Hybrid Web Security Mode, page 2-1](#)
- [About Policy Application from Cloud Web Security, page 2-1](#)
- [WSA Functionality Not Available in Hybrid Mode, page 2-2](#)
- [Pre-configuration Requirements, page 2-2](#)
- [What To Do Next, page 2-3](#)

## Overview of Hybrid Web Security Mode

Hybrid Web Security mode provides unified cloud and on-premise policy enforcement and threat defense, using policies defined in Cisco ScanCenter—the administrative portal to Cloud Web Security—which are automatically downloaded to the Web Security appliance.

Hybrid Web Security provides a subset of the features provided in Standard mode, and use of these is the same as in Standard mode, except as noted in this documentation. See [Comparison of Modes of Operation, page 3-2](#) for additional information.

This chapter 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 Hybrid Web Security mode. This chapter includes information about configuring the Hybrid Web Security that is not applicable in Standard mode.

This document does not include information about Cisco Cloud Web Security and ScanCenter. That documentation is available at

<http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html>.

## About Policy Application from Cloud Web Security

Please note these points regarding download, conversion and application of CWS policies/filters/rules to WSA policies:

- Translation of both default and user-defined CWS policies to WSA policies is not a one-to-one conversion; however, the action that results from application of a particular policy in both environments is the same. In other words, the Block or Allow decision is always consistent, regardless of the sequence of rules “fired” in both cases. This allows rule evaluation in the proxy to be optimized for better performance without compromising consistent behavior.

### ■ WSA Functionality Not Available in Hybrid Mode

- Supported anti-malware scanning services are not the same on both platforms; they will remain independent. The WSA provides an option to choose scanning services, and at least one must be enabled.
- In Hybrid mode, the WSA does not support the following items; these will not be downloaded:
  - Any rule assigned the Authenticate action.
  - Outbound filters. Any rule using a filter that contains any Keyword, Outbound File Type, Preconfigured ID, or Regular Expression. Inbound Extensions are also not supported.
  - Whitelisting sets of domains and URLs to bypass Sypware/Web Reputation scanning at the global level is not supported.
  - Anonymize. Any CWS rule that has the action set to Anonymize.
  - SearchAhead
  - WSA does not incorporate the concept of delegated administration. CWS will send the merged policy configuration.

## WSA Functionality Not Available in Hybrid Mode

The following WSA features are not available in Hybrid mode:

- Time and Volume Quotas
- External DLP
- SaaS Policies
- L4TM
- Upstream Proxy support
- ISE integration
- Range Requests
- Native FTP & SOCKS protocol support
- SNMP
- HTTPS rules assigned the Drop action

## Pre-configuration Requirements

- For compatibility with Cloud Web Security policies, when operating in Web Hybrid mode at least one anti-malware scanning engine (McAfee, Sophos, or Webroot) must be licensed and available. Ensure the valid license(s) or feature key(s) are available in order to complete set-up in Web Hybrid mode.
- Both CWS and WSA require a Certificate Authority-signed certificate to authenticate and secure communications between them. You must generate this certificate externally and upload the certificate and its key to both Cisco ScanCenter and the Cisco WSA. See [Uploading a Certificate and Key, page 12-25](#).
- Register this Web Security appliance with Cisco Cloud Web Security to obtain an authorization token. Be aware that this token is valid for one hour; if you have not used it to configure the WSA within that time, you will have to generate another. See [Registration with Cisco Cloud Web Security, page 3-9](#).

# What To Do Next

- Connect, install and configure the appliance in Hybrid Web Security mode. Refer to [Task Overview for Connecting, Installing, and Configuring, page 3-6](#) for specific information.
- As mentioned in [About Policy Application from Cloud Web Security, page 2-1](#), if any CWS policies to be downloaded contain HTTPS rules or authentication group rules, it is important that you configure HTTPS proxy settings, Authentication Realms and Identification Profiles on the WSA shortly after the System Setup Wizard (SSW) finishes configuring Hybrid Web Security mode. Conversion and download of any CWS policies containing HTTPS rules or authentication group rules is skipped during WSA hybrid system set-up, and will be completed only after the WSA is set up in hybrid mode with HTTPS proxy, Authentication Realms and Identification Profiles configured. (The conversion/download process is completed automatically, as CWS-to-WSA policy updates occur every two minutes.)

In CWS, an authentication realm refers to SAML and EasyID. On the WSA, the types supported are different and usually refer to NTLM (SAML is not yet supported on the WSA). If CWS rules have either auth-user-name or authentication groups configured, you must configure authentication realms and custom identification profiles with authentication enabled on the WSA.

- Configure HTTPS proxy settings: see [Enabling the HTTPS Proxy, page 7-3](#).
- Configure Authentication Realms and Identification Profiles: see [Classify End-Users and Client Software, page 6-1](#).
- The Acceptable Use Policy (AUP) page on CWS and the End-User Acknowledgment (EUA) page on the WSA are essentially the same thing: a page displayed to end-users explaining terms of access, which users are required to click to acknowledge before proceeding.

If you are using this option on CWS, you should also enable it locally on the WSA (Security Services > End-User Notification) to provide the same required behavior for all end users. The EUA settings must be configured locally on the WSA—they are not downloaded from CWS. You can edit the HTML presented to end-users by the WSA to ensure that both pages have a similar “look and feel.”
- Some items that are configurable in Cisco ScanCenter are not yet supported for download by the Web Security appliance. The following items must be configured directly on the appliance:
  - Email Alert Settings. Frequency of email alerts you want to receive. (An email address is provided during configuration with the Software Setup Wizard; others can be added later.)
  - Customized text and other settings for Block pages and end-user alert pages.
  - Global settings such as SearchAhead, SafeSearch, Dynamic Classification Engine, Content Range Headers, and Sandboxing.
- Note that when the WSA Hybrid software is installed or upgraded it will likely have an AVC Signature version that does not match that of the CWS service. The WSA will not generate rules for those applications for which there is a mismatch, but will generate rules for all matching signatures. Signature mismatches that cannot be applied are logged. (The correct AVC Signature file will be downloaded, generally after no more than 10 minutes.)
- Logging: `hybriddd` logs are enabled as part of Hybrid mode, and the level can be configured like all other WSA logs. Consult the `hybriddd` and `configdefragd` logs if you encounter errors during policy conversion.

**■ What To Do Next**



## Connect, Install, and Configure

- [Overview of Connect, Install, and Configure, page 3-1](#)
- [Deploying a Virtual Appliance, page 3-2](#)
- [Comparison of Modes of Operation, page 3-2](#)
- [Task Overview for Connecting, Installing, and Configuring, page 3-6](#)
- [Connecting the Appliance, page 3-6](#)
- [Gathering Setup Information, page 3-8](#)
- [System Setup Wizard, page 3-10](#)
- [Upstream Proxies, page 3-17](#)
- [Network Interfaces, page 3-19](#)
- [Configuring Failover Groups for High Availability, page 3-21](#)
- [Using the P2 Data Interface for Web Proxy Data, page 3-22](#)
- [Redirect Hostname and System Hostname, page 3-31](#)
- [DNS Settings, page 3-33](#)
- [Troubleshooting Connect, Install, and Configure, page 3-35](#)

## Overview of Connect, Install, and Configure

The Web Security appliance provides three modes of operation: Standard, Cloud Web Security Connector, and Hybrid Web Security.

The Standard mode of Web Security appliance operation includes on-site Web proxy services, which is not available in Cloud Web Security Connector mode, and Layer-4 traffic monitoring, which is not available in either Hybrid Web Security or Cloud Web Security Connector modes.

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.

Hybrid Web Security mode provides unified cloud and on-premise policy enforcement and threat defense, using policies defined in Cisco ScanCenter—the administrative portal to Cloud Web Security—which are automatically downloaded to the Web Security appliance.

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 Standard mode of Web Security Appliance operation includes on-site Web proxy services, which is not available in Cloud Web Security Connector mode, and Layer-4 traffic monitoring, which is not available in either Hybrid Web Security or Cloud Web Security Connector modes.

In Cloud Web Security Connector mode, the appliance connects to and routes traffic to a Cisco Cloud Web Security proxy, where Web security policies are enforced.

Hybrid Web Security mode provides both cloud and on-premise policy enforcement and threat defense by incorporating connection to a Cisco Cloud Web Security proxy.

The following table presents the various menu commands available in each mode, thereby indicating the various features available in each mode.

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

**Comparison of Modes of Operation**

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

Menu	Available in Standard Mode	Available in Cloud Connector Mode	Available in Hybrid Web Security Mode
<b>Network</b>	Interfaces	Interfaces	Interfaces
	Transparent Redirection	Transparent Redirection	Transparent Redirection
	Routes	Routes	Routes
	DNS	DNS	DNS
	High Availability	High Availability	High Availability
	Internal SMTP Relay	Internal SMTP Relay	Internal SMTP Relay
	Upstream Proxy	External DLP Servers	Certificate Management
	External DLP Servers	Certificate Management	Authentication
	Certificate Management	Authentication	
	Authentication	Machine ID Service	
<b>System Administration</b>	Identity Provider for SaaS	Cloud Connector	
	Identity Services Engine		
<b>Cisco CWS Portal (available only in Hybrid Web Security mode)</b>	Policy Trace	Alerts	Alerts
	Alerts	Log Subscriptions	Log Subscriptions
	Log Subscriptions	SSL Configuration	SSL Configuration
	Return Addresses	Users	Users
	SSL Configuration	Network Access	Network Access
	Users	Time Zone	Time Zone
	Network Access	Time Settings	Time Settings
	Time Zone	Configuration Summary	Configuration Summary
	Time Settings	Configuration File	Configuration File
	Configuration Summary	Feature Keys	Feature Key Settings
	Configuration File	Upgrade and Update Settings	Feature Keys
	Feature Keys Settings	System Upgrade	Upgrade and Update Settings
	Feature Keys	System Setup Wizard	System Setup Wizard
	Upgrade and Update Settings		Next Steps
	System Upgrade		
	System Setup Wizard		
	FIPS Mode		
	Next Steps		

# Task Overview for Connecting, Installing, and Configuring

Task	More Information
1. Connect the appliance to Internet traffic.	<a href="#">Connecting the Appliance, page 3-6</a>
2. Gather and record set-up information.	<a href="#">Gathering Setup Information, page 3-8</a>
3. Run the System Setup Wizard.	<a href="#">System Setup Wizard, page 3-10</a>
4. Configure HTTPS proxy settings, Authentication Realms and Identification Profiles.  <b>This step must be completed for Hybrid Web Security mode.</b>	<a href="#">Enabling the HTTPS Proxy, page 7-3</a> <a href="#">Authentication Realms, page 5-10</a> <a href="#">Identification Profiles and Authentication, page 6-7</a>
5. (Optional) Connect upstream proxies.	<a href="#">Upstream Proxies, page 3-17</a>

## Connecting 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, page C-2](#).
- If you plan to physically connect the appliance to a WCCP v2 router for transparent redirection, first verify that the WCCP router supports Layer 2 redirection.
- Be aware of Cisco configuration recommendations:
  - Use simplex cabling (separate cables for incoming and outgoing traffic) if possible for enhanced performance and security.

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

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

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

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

**Step 3** 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, page 3-8](#)

#### Related Topics

- [Enabling or Changing Network Interfaces, page 3-19](#)
- [Using the P2 Data Interface for Web Proxy Data, page 3-22](#)
- [Adding and Editing a WCCP Service, page 3-26](#)
- [Configuring Transparent Redirection, page 3-25](#)
- [Upstream Proxies, page 3-17](#)

# Gathering Setup Information

You can use the worksheet below to record the configuration values you will need while running the System Setup Wizard. For additional information about each property, see [System Setup Wizard Reference Information](#), page 3-12.

**System Setup Wizard Worksheet**

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

## Registration with Cisco Cloud Web Security

A Web Security appliance operating in Hybrid Web Security mode must be registered with Cisco Cloud Web Security (CWS) in order to download and periodically update security policies from the cloud.

Upon successful registration, the security appliance downloads your Cisco Cloud Web Security policy from Cisco ScanCenter.

- Every time you modify your CWS policy in Cisco ScanCenter, the whole policy is downloaded to the security appliance to synchronize policies.
- By default, the appliance checks every two minutes to determine if an updated policy is available for download.
- The **Reporting > System Status** displays the status of Hybrid mode registration with CWS.

Follow these steps to register with CWS and generate a connection token for the WSA.

---

**Step 1** Log into your Cisco ScanCenter account.

**Step 2** Click the **Admin** tab.

**Step 3** Choose **Management > Hybrid Web Security**.

**Step 4** Click **Generate Token**.

**Step 5** When the new token appears, click **Copy Token to Clipboard**.

---

### What's Next

Paste this token in the Enter Authorization Key dialog box on the Web Policy Connectivity page of the Web Security appliance's System Software Wizard, as described in [System Setup Wizard, page 3-10](#).

Be aware that this token is valid for one hour; if you have not used it to configure the WSA within that time, you will have to generate another.

### Related Topics

- [http://www.cisco.com/c/en/us/td/docs/security/web\\_security/scancenter/administrator/guide/b\\_Scan\\_Center\\_Administrator\\_Guide.html](http://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_Scan_Center_Administrator_Guide.html)

## Changing Registration on the Web Security appliance

To change or update your Cisco ScanCenter registration on the WSA:

---

**Step 1** Choose **Network > Web Policy Connectivity**.

**Step 2** Click **Change Registration**.

**Step 3** Enter the new authorization token you received from the Cisco ScanCenter portal in the Enter Authorization Key dialog box and then click **Register**.

---

# System Setup Wizard

## Before You Begin:

- Connect the Appliance to networks and devices. See [Connecting the Appliance, page 3-6](#).
- Complete the System Setup Wizard worksheet. See [Gathering Setup Information, page 3-8](#).
- 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.
- In order to set up Web Hybrid mode, it is necessary to run the System Setup Wizard to configure the appliance in Standard mode, then upgrade to AsyncOS 9.2, and then re-run the System Setup Wizard to configure in Hybrid Web Security mode. (This does not apply to virtual images that are not being upgraded.)
- For compatibility with Cloud Web Security policies, when operating in Web Hybrid mode at least one anti-malware scanning engine (McAfee, Sophos, or Webroot) must be licensed and available. Ensure the valid license(s) or feature key(s) are available in order to complete set-up in Web Hybrid mode.
- Both CWS and WSA require a Certificate Authority-signed certificate to authenticate and secure communications between them. You must generate this certificate externally and upload the certificate and its key to both Cisco ScanCenter and the Cisco WSA. See [Uploading a Certificate and Key, page 12-25](#).
- Register this Web Security appliance with Cisco Cloud Web Security to obtain an authorization token. Be aware that this token is valid for one hour; if you have not used it to configure the WSA within that time, you will have to generate another. See [Registration with Cisco Cloud Web Security, page 3-9](#).
- Note that reference information for each configuration item used in the System Setup Wizard is available at [System Setup Wizard Reference Information, page 3-12](#).



**Only use the System Setup Wizard the first time you install the appliance, or if you want to completely overwrite the existing configuration. Note that the appliance will be reset to its initial factory defaults even if you cancel the System Setup Wizard before it is complete.**

## 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, page 3-12](#).

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

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

**Step 10** Connect the appliance to Cisco Cloud Web Security for Hybrid Web Security policy communications:

- a. Click **Register** on the Web Policy Connectivity page of the System Software Wizard.
- b. Enter the authorization token you copied from the Cisco ScanCenter portal in the Enter Authorization Key dialog box and then click Register.

See [Registration with Cisco Cloud Web Security, page 3-9](#) for more about obtaining an authorization token.

See [Changing Registration on the Web Security appliance, page 3-9](#) for information about changing this authorization token.

Upon successful registration, available security policies are downloaded from Cisco ScanCenter to the Web Security appliance. See [About Policy Application from Cloud Web Security, page 2-1](#) for additional information.

---

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.

### What to Do Next

If any CWS policies to be downloaded contain HTTPS rules or authentication group rules, it is important that you configure HTTPS proxy settings, Authentication Realms and Identification Profiles on the WSA shortly after the System Setup Wizard (SSW) finishes configuring Hybrid Web Security mode. Conversion and download of any CWS policies containing HTTPS rules or authentication group rules are skipped during WSA hybrid system set-up, and will be completed only after the WSA is set up in hybrid mode, with HTTPS proxy, Authentication Realms and Identification Profiles configured. (The conversion/download process is completed automatically, as CWS-to-WSA policy updates occur every two minutes.)

**System Setup Wizard**

In CWS, an authentication realm refers to SAML and EasyID. On the WSA, the types supported are different and usually refer to NTLM (SAML is not yet supported on the WSA). If CWS rules have either auth-user-name or authentication groups configured, you must configure authentication realms and custom identification profiles with authentication enabled on the WSA.

- Configure HTTPS proxy settings: see [Enabling the HTTPS Proxy, page 7-3](#).
- Configure Authentication Realms and Identification Profiles: see [Classify End-Users and Client Software, page 6-1](#).

In addition, some items that are configurable in Cisco ScanCenter are not yet supported for download by the Cisco Web Security appliance. The following items must be configured directly on the appliance:

- Email Alert Settings. Frequency of email alerts you want to receive. (Email addresses are provided during configuration with the Software Setup Wizard.)
- Customized Alerts. Custom alert pages for Blocks and Warns or AUP custom text.
- Global Settings. Enabling of settings such as SearchAhead, SafeSearch, AUP (EUA on the WSA), Dynamic Classification Engine, Content Range Headers, and Sandboxing.

## System Setup Wizard Reference Information

- [Network / System Settings, page 3-13](#)
- [Network / Network Interfaces and Wiring, page 3-14](#)
- [Network / Routes for Management and Data Traffic, page 3-15](#)
- [Network / Transparent Connection Settings, page 3-15](#)
- [Network / Administrative Settings, page 3-16](#)
- [Security / Upgrade Timing, page 3-17](#)

## Network / System Settings

Property	Description
Default System Hostname	<p>The system hostname is the fully-qualified hostname used to identify the appliance in the following areas:</p> <ul style="list-style-type: none"> <li>• the command line interface (CLI)</li> <li>• system alerts</li> <li>• end-user notification and acknowledgment pages</li> <li>• when forming the machine NetBIOS name when the Web Security appliance joins an Active Directory domain</li> </ul> <p>The system hostname does not correspond directly to interface hostnames and is not used by clients to connect to the appliance.</p>
DNS Server(s)	<ul style="list-style-type: none"> <li>• <b>Use the Internet's Root DNS Servers</b> – 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.</li> </ul> <p><b>Note</b> 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.</p> <p><b>Use these DNS Servers</b> – Provide address(es) for the local DNS server(s) that the appliance can use to resolve host names.</p> <p>See <a href="#">DNS Settings, page 3-33</a> for more information about these settings.</p>
NTP Server	<p>The Network Time Protocol (NTP) server used to synchronize the system clock with other servers on the network or the Internet.</p> <p>The default is time.sco.cisco.com.</p>
Time Zone	<p>Provide time-zone information for location of the appliance; affects timestamps in message headers and log files.</p>
Appliance Mode of Operation	<ul style="list-style-type: none"> <li>• Standard – Used for standard on-premise policy enforcement.</li> <li>• Cloud Web Security Connector – Used primarily to direct traffic to Cisco's Cloud Web Security service for policy enforcement and threat defense.</li> <li>• Hybrid Web Security – Used in conjunction with Cisco's Cloud Web Security service for cloud and on-premise policy enforcement and threat defense.</li> </ul> <p>See <a href="#">Comparison of Modes of Operation, page 3-2</a> for more information about these modes of operation.</p>

## Network / 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 <b>Connect directly</b> to the Internet, or <b>Drop requests</b> .
Cloud Web Security Authorization Scheme	Method for authorizing transactions: <ul style="list-style-type: none"> <li>• Web Security Appliance public-facing IPv4 address.</li> <li>• Authorization key included with each transaction. You can generate an authorization key within the Cisco Cloud Web Security Portal.</li> </ul>

## 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 <b>Use M1 port for management only</b> if you want to use a separate port for data traffic.  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.  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 / 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.
Static Routes Table	Optional static routes for management and data traffic. Multiple routes can be added. <ul style="list-style-type: none"> <li>• <b>Name</b> – A name used to identify the static route.</li> <li>• <b>Internal Network</b> – The IPv4 address for this route’s destination on the network.</li> <li>• <b>Internal Gateway</b> – 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.</li> </ul>

## 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. <p>If you connect the appliance to a version 2 WCCP router, you must create at least one WCCP service. You can enable the standard service on this screen, or after the System Setup Wizard is finished, where you can also create multiple dynamic services.</p> <p>When you enable the standard service, you can also enable router security and enter a passphrase. The passphrase used here must be used all appliances and WCCP routers within the same service group.</p> <p>A standard service type (also known as the “web-cache” service) is assigned a fixed ID of zero, a fixed redirection method (by destination port), and a fixed destination port of 80.</p> <p>A dynamic service type allows you to define a custom ID, port numbers, and redirection and load balancing options.</p>

## Network /Administrative Settings

Property	Description
Administrator Passphrase	The passphrase used to access the Web Security appliance for administrative purposes.
Email System Alerts To	The email address to which the appliance sends systems alerts.
Send Email via SMTP Relay Host (optional)	The address and port for an SMTP relay host that AsyncOS can use to send system generated email messages. 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.  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
Malware and Spyware Scanning	Specifies whether to enable malware and spyware scanning using Webroot, McAfee, or Sophos. 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.  If any option is enabled, also choose whether to monitor or block detected malware. The default setting is to monitor malware.  You can further configure malware scanning after you finish the System Setup Wizard.

## Security / Upgrade Timing

Option	Description
Upgrade Timing Windows	<p>In Hybrid mode, upgrades are downloaded automatically whenever available, and then installed during a specified time window. At least two time windows per week must be specified to allow performance of required software updates. These timings must be:</p> <ul style="list-style-type: none"> <li>• At least two hours long.</li> <li>• No more than four days apart (for instance, if the first selection is Monday, the second may be Thursday or Friday).</li> </ul> <p>For each time window, choose the day of week, start time, and duration. You are defining the start of a two-hour window during which upgrades/updates installation may begin. Since the appliance will reboot when installation is completed, specify the least-disruptive time possible.</p> <p><b>Note</b> Do not configure an upgrade time window that is within 30 minutes of registering this WSA with the CWS portal—that is, not within 30 minutes of completing the final step of the System Setup Wizard.</p> <p>See <a href="#">AsyncOS for Web Upgrades and Updates, page 12-27</a> for information about changing the time window, and for setting a one-time exception to this window.</p>

## Upstream Proxies

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

- [Upstream Proxies Task Overview, page 3-17](#)
- [Creating Proxy Groups for Upstream Proxies, page 3-17](#)

## Upstream Proxies Task Overview

Task	More Information
1. Connect the external proxy upstream of the Cisco Web Security Appliance.	<a href="#">Connecting the Appliance, page 3-6.</a>
2. Create and configure a proxy group for the upstream proxy.	<a href="#">Creating Proxy Groups for Upstream Proxies, page 3-17.</a>
3. Create a routing policy for the proxy group to manage which traffic is routed to the upstream proxy.	<a href="#">Create Policies to Control Internet Requests</a>

## Creating Proxy Groups for Upstream Proxies

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

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

**Step 3** Complete the Proxy Group settings.

Property	Description
<b>Name</b>	The name used to identify proxy groups on the appliance, such as in routing policies, for example.
<b>Proxy Servers</b>	<p>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.</p> <p><b>Note</b> You can enter the same proxy server multiple times to allow unequal load distribution among the proxies in the proxy group.</p>
<b>Load Balancing</b>	<p>The strategy that the web proxy uses to load balance requests between multiple upstream proxies. Choose from:</p> <ul style="list-style-type: none"> <li>• <b>None (failover).</b> 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.</li> <li>• <b>Fewest connections.</b> 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.</li> <li>• <b>Hash based. Least recently used.</b> 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.</li> <li>• <b>Round robin.</b> The Web Proxy cycles transactions equally among all proxies in the group in the listed order.</li> </ul> <p><b>Note</b> The Load Balancing option is dimmed until two or more proxies have been defined.</p>
<b>Failure Handling</b>	<p>Specifies the default action to take if all proxies in this group fail. Choose from:</p> <ul style="list-style-type: none"> <li>• <b>Connect directly.</b> Send the requests directly to their destination servers.</li> <li>• <b>Drop requests.</b> Discard the requests without forwarding them.</li> </ul>

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

#### What to Do Next.

- [Creating a Policy, page 10-7](#)

# Network Interfaces

- [IP Address Versions, page 3-19](#)
- [Enabling or Changing Network Interfaces, page 3-19](#)

## IP Address Versions

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



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

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

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

### Related Topics

- [Enabling or Changing Network Interfaces, page 3-19](#)
- [DNS Settings, page 3-33](#)

## Enabling or Changing Network Interfaces

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

---

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

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

**Step 3** Configure the Interface options .

Option	Description
Interfaces	<p>Modify or add new IPv4 or IPv6 Address, Netmask, and Hostname details for the M1, P1, or P2 interfaces as required.</p> <ul style="list-style-type: none"> <li>• <b>M1</b> – 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.</li> <li>• <b>P1 and P2</b> – 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.</li> </ul> <p><b>Note</b> If the Management and Data interfaces are all configured, each must be assigned IP addresses on different subnets.</p>
Separate Routing for Management Services	<p>Check <b>Restrict M1 port to appliance management services only</b> to limit M1 to management traffic only, requiring use of a separate port for data traffic.</p> <p><b>Note</b> When you use M1 for management traffic only, configure at least one data interface, on another subnet, for proxy traffic. Define different routes for management and data traffic.</p>
Appliance Management Services	<p>Enable/disable use of, and specify a default port number for, the following network protocols:</p> <ul style="list-style-type: none"> <li>• <b>FTP</b> – Disabled by default.</li> <li>• <b>SSH</b></li> <li>• <b>HTTP</b></li> <li>• <b>HTTPS</b></li> </ul> <p>Also, you can enable/disable redirection of HTTP traffic to HTTPS.</p>

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

#### What to Do Next

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

#### Related Topics

- [Connecting the Appliance, page 3-6](#).
- [IP Address Versions, page 3-19](#)
- [Configuring TCP/IP Traffic Routes, page 3-23](#)

# Configuring Failover Groups for High Availability

Using the Common Address Redundancy Protocol (CARP), the WSA enables multiple hosts on your network to share an IP address, providing IP redundancy to ensure high availability of services provided by those hosts. In CARP there are three states for a host:

- master
- backup
- init

Only one master host can exist for each failover group that can provide services.

## 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.

---

**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 **Master** 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.
- 

#### Related Topics

- [Failover Problems, page A-3](#)

## Edit High Availability Global Settings

- 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, page 3-19](#)).

---

**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.

---

#### Related Topics

- [Connecting the Appliance, page 3-6.](#)
- [Configuring TCP/IP Traffic Routes, page 3-23.](#)

## 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
<ul style="list-style-type: none"> <li>• WebUI</li> <li>• SSH</li> <li>• SNMP</li> <li>• NTLM authentication (with domain controller)</li> <li>• ICAP request with external DLP server</li> <li>• Syslogs</li> <li>• FTP push</li> <li>• DNS (configurable)</li> <li>• Update/Upgrade/Feature Key (configurable)</li> </ul>	<ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> <li>• FTP</li> <li>• WCCP negotiation</li> <li>• DNS (configurable)</li> <li>• Update/Upgrade/Feature Key (configurable)</li> </ul>

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.

#### Related Topics

- To enable split routing of management and data traffic, see [Enabling or Changing Network Interfaces, page 3-19](#)

## Modifying the Default Route

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

## Adding a Route

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

## Saving and Loading Routing Tables

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



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

## Deleting a Route

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

### Related Topics

- [Enabling or Changing Network Interfaces, page 3-19](#).

## Configuring Transparent Redirection

### Specifying a Transparent Redirection Device

#### Before You Begin

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

- 
- Step 1** Choose **Network > Transparent Redirection**.
- Step 2** Click **Edit Device**.

## Using the P2 Data Interface for Web Proxy Data

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

### Related Topics

- [Connecting the Appliance, page 3-6.](#)
- [Configuring WCCP Services, page 3-26.](#)

## 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.



**Note** You can configure a maximum of 15 service groups on a single appliance.

### Adding and Editing a WCCP Service

#### Before You Begin

- Configure the appliance to use a WCCP v2 Router (see [Specifying a Transparent Redirection Device, page 3-25](#)).

- 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.  <b>Note</b> If you leave this empty and choose a standard service (see below), the name ‘web_cache’ is automatically assigned here.

WCCP Service Option	Description
Service	<p>The service group type for the router. Choose from:</p> <p><b>Standard service.</b> This service type is assigned a fixed ID of zero, a fixed redirection method of <i>by destination port</i>, and a fixed destination port of 80. You can create one standard service only. If a standard service already exists on the appliance, this option is dimmed.</p> <p><b>Dynamic service.</b> This service type allows you to define a custom ID, port numbers, and redirection and load balancing options. Enter the same parameters when creating the service on the WCCP router as you entered for the dynamic service.</p> <p>If you create a dynamic service, enter the following information:</p> <ul style="list-style-type: none"> <li>• <b>Service ID.</b> 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.</li> <li>• <b>Port number(s).</b> Enter up to eight port numbers for traffic to redirect in the Port Numbers field.</li> <li>• <b>Redirection basis.</b> Choose to redirect traffic based on the source or destination port. Default is destination port.</li> </ul> <p> <b>Note</b> To configure Native FTP with transparent redirection and IP spoofing, choose Redirect based on source port (return path) and set the source port to 13007.</p> <ul style="list-style-type: none"> <li>• <b>Load balancing basis.</b> When the network uses multiple Web Security appliances, you can choose how to distribute packets among the appliances. You can distribute packets based on the server or client address. When you choose client address, packets from a client always get distributed to the same appliance. Default is server address.</li> </ul>
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	Specifies whether or not 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.

WCCP Service Option	Description
Advanced	<p><b>Load-Balancing Method.</b> This determines how the router performs load balancing of packets among multiple Web Security appliances. Choose from:</p> <ul style="list-style-type: none"> <li>• <b>Allow Mask Only.</b> 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.</li> <li>• <b>Allow Hash Only.</b> 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.</li> <li>• <b>Allow Hash or Mask.</b> Allows AsyncOS to negotiate a method with the router. If the router supports mask, then AsyncOS uses masking, otherwise hashing is used.</li> </ul> <p><b>Mask Customization.</b> If you select Allow Mask Only or Allow Hash or Mask, you can customize the mask or specify the number of bits:</p> <ul style="list-style-type: none"> <li>• <b>Custom mask (max 5 bits).</b> You can specify the mask. The web interface displays the number of bits associated with the mask you provide.</li> <li>• <b>System generated mask.</b> You can let the system generate a mask for you. Optionally, you can specify the number of bits for the system-generated mask, up to 5 bits.</li> </ul> <p><b>Forwarding method.</b> This is the method by which redirected packets are transported from the router to the web proxy.</p> <p><b>Return Method.</b> This is the method by which redirected packets are transported from the web proxy to the router.</p> <p>Both the forwarding and return methods use one of the following method types:</p> <ul style="list-style-type: none"> <li>• <b>Layer 2 (L2).</b> 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.</li> <li>• <b>Generic Routing Encapsulation (GRE).</b> 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.</li> <li>• <b>L2 or GRE.</b> 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.</li> </ul> <p>If the router is not directly connected to the appliance, you must choose GRE.</p>

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

## Creating WCCP Services for IP Spoofing

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

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

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



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

### Related Topics

- [Web Proxy Cache, page 4-5.](#)

## 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.

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

## Configuring and Managing VLANs

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

### Example 1: Creating a New VLAN

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



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

**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.
```

**Using the P2 Data Interface for Web Proxy Data**

```

- MTU - View and configure MTU.
[]> vlan

VLAN interfaces:

Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new

VLAN ID for the interface (Ex: "34"):
[]> 34

Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2

VLAN interfaces:
1. VLAN 34 (P1)

Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]> new

VLAN ID for the interface (Ex: "34"):
[]> 31

Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2

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

Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]>

```

**Step 3** Commit your changes.**Example 2: Creating an IP Interface on a VLAN**

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

**Note**

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

**Step 1** Access the CLI.

**Step 2** Follow the steps shown:

```
example.com> interfaceconfig

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

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- 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 "0xffffffff00"):
[255.255.255.0]>

Hostname:
[]> v.example.com

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

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>

example.com> commit
```

**Step 3** Commit your changes.

---

#### Related Topics

- [Enabling or Changing Network Interfaces, page 3-19.](#)
- [Configuring TCP/IP Traffic Routes, page 3-23.](#)

## 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.

## ■ Redirect Hostname and System Hostname

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

- The command line interface (CLI)
- System alerts
- When forming the machine NetBIOS name when the Web Security appliance joins an Active Directory domain.

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

## Changing the Redirect Hostname

---

**Step 1** In the web user interface, navigate to **Network>Authentication**.

**Step 2** Click Edit Global Settings.

**Step 3** Enter a new value for Redirect Hostname.

---

## Changing the System Hostname

---

**Step 1** Access the CLI.

**Step 2** Use the `sethostname` command to change the name of the Web Security appliance:

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

**Step 3** Commit your changes.

---

## Configuring SMTP Relay Host Settings

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




---

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

---

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

## Configuring an SMTP Relay Host

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

**Step 2** Click Edit Settings.

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

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

**Step 4** (Optional) Click Add Row to add additional SMTP relay hosts.

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

## DNS Settings

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

- [Split DNS, page 3-33](#)
- [Clearing the DNS Cache, page 3-33](#)
- [Editing DNS Settings, page 3-34](#)

## Split DNS

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

## Clearing the DNS Cache

### Before You Begin

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

**Step 1** Choose Network > DNS.

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

---

## Editing DNS Settings

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

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

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

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

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

---

### Related Topics

- [Configuring TCP/IP Traffic Routes, page 3-23](#)
- [IP Address Versions, page 3-19](#)

# Troubleshooting Connect, Install, and Configure

- Failover Problems, page A-3
- Upstream Proxy Does Not Receive Basic Credentials, page A-14
- Client Requests Fail Upstream Proxy, page A-14
- Maximum Port Entries, page A-15

**Troubleshooting Connect, Install, and Configure**



## Intercepting Web Requests

---

- [Overview of Intercepting Web Requests, page 4-1.](#)
- [Tasks for Intercepting Web Requests, page 4-2.](#)
- [Best Practices for Intercepting Web Requests, page 4-2.](#)
- [Web Proxy Options for Intercepting Web Requests, page 4-3.](#)
- [Client Options for Redirecting Web Requests, page 4-10.](#)

## 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, and other proxy servers or Web Security appliances.

# Tasks for Intercepting Web Requests

Steps	Task	Links to Related Topics and Procedures
1.	Review best practices.	<ul style="list-style-type: none"> <li>Best Practices for Intercepting Web Requests, page 4-2</li> </ul>
2.	(Optional) Perform follow up networking tasks: <ul style="list-style-type: none"> <li>Connect and configure upstream proxies.</li> <li>Configure network interface ports.</li> <li>Configure transparent redirection devices.</li> <li>Configure TCP/IP routes.</li> <li>Configure VLANs.</li> </ul>	<ul style="list-style-type: none"> <li>Upstream Proxies, page 3-17</li> <li>Network Interfaces, page 3-19</li> <li>Configuring Transparent Redirection, page 3-25</li> <li>Configuring TCP/IP Traffic Routes, page 3-23</li> <li>Increasing Interface Capacity Using VLANs, page 3-29</li> </ul>
3.	(Optional) Perform follow up Web Proxy tasks: <ul style="list-style-type: none"> <li>Configure the web proxy to operate in either Forward or Transparent mode.</li> <li>Decide if additional services are needed for the protocol types you want to intercept</li> <li>Manage the web proxy cache.</li> <li>Use custom web request headers.</li> <li>Bypass the proxy for some requests.</li> </ul>	<ul style="list-style-type: none"> <li>Web Proxy Options for Intercepting Web Requests, page 4-3</li> <li>Configuring Web Proxy Settings, page 4-3</li> <li>Web Proxy Options for Intercepting Web Requests, page 4-3</li> <li>Web Proxy Cache, page 4-5</li> <li>Web Proxy Bypassing, page 4-9</li> </ul>
4.	Perform client tasks: <ul style="list-style-type: none"> <li>Decide how clients should redirect requests to the web proxy.</li> <li>Configure clients and client resources.</li> </ul>	<ul style="list-style-type: none"> <li>Client Options for Redirecting Web Requests, page 4-10</li> <li></li> </ul>

## 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:

- **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.

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.

## Configuring Web Proxy Settings

### Before You Begin

- Enable the web proxy.

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

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

**Step 3** Configure the basic web proxy settings as required.

Property	Description
HTTP Ports to Proxy	The ports that the web Proxy will listen on for HTTP connections
HTTP CONNECT Ports	The ports applications are allowed to use for tunneling outbound traffic over HTTP.
Caching	Specifies whether to enable or disable Web Proxy caching. The web proxy caches data to increase performance.
Proxy mode	<ul style="list-style-type: none"><li>• <b>Forward</b> — 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.</li><li>• <b>Transparent (Recommended)</b> — Allow the web proxy to name the internet target. The web proxy can intercept both transparent and explicitly forwarded web requests in this mode.</li></ul>

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

Property	Description
Persistent Connection Timeout	<p>The maximum time in seconds the web proxy keeps open a connection to a client or server after a transaction has been completed and no further activity is detected.</p> <ul style="list-style-type: none"> <li>• <b>Client side.</b> The timeout value for connections to clients.</li> <li>• <b>Server side.</b> The timeout value for connections to servers.</li> </ul> <p>If you increase these values connections will remain open longer and reduce the overhead used to open and close connections repeatedly. However, you also reduce the ability of the Web Proxy to open new connections if the maximum number of simultaneous persistent connections has been reached. Cisco recommends keeping the default values.</p>
In-Use Connection Timeout	<p>The maximum time in seconds that the web proxy waits for more data from an idle client or server when the current transaction has not yet been completed.</p> <ul style="list-style-type: none"> <li>• <b>Client side.</b> The timeout value for connections to clients.</li> <li>• <b>Server side.</b> The timeout value for connections to servers.</li> </ul>
Simultaneous Persistent Connections (Server Maximum Number)	The maximum number of connections (sockets) the Web Proxy keeps open with servers.
Generate Headers	<p>Generate and add headers that encode information about the request.</p> <ul style="list-style-type: none"> <li>• <b>X-Forwarded-For</b> headers encode the IP address of the client from which an HTTP request originated.</li> </ul> <p> <b>Note</b> To turn header forwarding on or off, use the CLI <code>advancedproxyconfig</code> command, Miscellaneous option, “Do you want to pass HTTP X-Forwarded-For headers?”</p> <p> <b>Note</b> Using an explicit forward upstream proxy to manage user authentication or access control with proxy authentication requires forwarding of these headers.</p> <ul style="list-style-type: none"> <li>• <b>Request Side VIA</b> headers encode the proxies through which the request passed on its way from the client to the server.</li> <li>• <b>Response Side VIA</b> headers encode the proxies through which the request passed on its way from the server to the client.</li> </ul>
Use Received Headers	<p>Allows a Web proxy deployed as an upstream proxy to identify clients using X-Forwarded-For headers send by downstream proxies. The Web Proxy will not accept the IP address in a X-Forwarded-For header from a source that is not included in this list.</p> <p>If enabled, requires the IP address of a downstream proxy or load balancer (you cannot enter subnets or host names).</p>

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

#### Related Topics

- [Web Proxy Cache, page 4-5.](#)
- [Configuring Transparent Redirection, page 3-25](#)

## 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

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

### Removing URLs from the Web Proxy Cache

- 
- Step 1** Access the CLI.
- Step 2** Use the `webcache > evict` commands to access the required caching area:

`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

- 
- Step 1** Access the CLI.
- Step 2** Use the `webcache -> ignore` commands to access the required submenus:

## ■ Web Proxy Options for Intercepting Web Requests

```
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, page 9-21](#) 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

---

**Step 1** Access the CLI.

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

```
example.com> advancedproxyconfig
```

Choose a parameter group:

```

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

```

Enter values for the caching options:

The following predefined choices exist for configuring advanced caching options:

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

Please select from one of the above choices:

[2]>

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

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

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

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

**Step 6** Commit your changes.

---

### Related Topics

- [Web Proxy Cache, page 4-5.](#)

## Web Proxy Custom Headers

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

### Adding Custom Headers To Web Requests

**Step 1** Access the CLI.

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

```
example.com> advancedproxyconfig
```

Choose a parameter group:

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

```
[ ]> customheaders
```

Currently defined custom headers:

Choose the operation you want to perform:

- DELETE - Delete entries
- NEW - Add new entries
- EDIT - Edit entries

```
[ ]>
```

**Step 3** Enter the required subcommand as follows:

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

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

- 
- Step 5** Commit your changes.
- 

## Web Proxy Bypassing

- [Web Proxy Bypassing for Web Requests, page 4-9](#)
- [Configuring Web Proxy Bypassing for Web Requests, page 4-9](#)
- [Configuring Web Proxy Bypassing for Applications, page 4-9](#)

### Web Proxy Bypassing for Web Requests

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

Bypassing the web proxy allows you to:

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

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

### Configuring Web Proxy Bypassing for Web Requests

---

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

### Configuring Web Proxy Bypassing for Applications

---

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

## Web Proxy Usage Agreement

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

### Related Topics

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

## Client Options for Redirecting Web Requests

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

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



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

## Troubleshooting Intercepting Requests

- [URL Categories Do Not Block Some FTP Sites, page A-4](#)
- [Large FTP Transfers Disconnect, page A-4](#)
- [Zero Byte File Appears On FTP Servers After File Upload, page A-5](#)
- [Unable to Route FTP Requests Via an Upstream Proxy, page A-14](#)
- [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, page A-10](#)
- [User Matches Global Policy for HTTPS and FTP over HTTP Requests, page A-11](#)



## Acquire End-User Credentials

- [Overview of Acquire End-User Credentials, page 5-1](#)
- [Authentication Best Practices, page 5-2](#)
- [Authentication Realms, page 5-10](#)
- [Failed Authentication, page 5-28](#)
- [Credentials, page 5-35](#)
- [Troubleshooting Authentication, page 5-37](#)

## Overview of Acquire End-User Credentials

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

## Authentication Task Overview

Step	Task	Links to Related Topics and Procedures
1.	Create an authentication realm.	<ul style="list-style-type: none"> <li>• <a href="#">How to Create an Active Directory Authentication Realm (NTLMSSP and Basic), page 5-14</a></li> <li>• <a href="#">Creating an LDAP Authentication Realm, page 5-16</a></li> </ul>
2.	Configure global authentication settings.	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Global Authentication Settings, page 5-21</a></li> </ul>
3.	Configure external authentication.  You can authenticate users through an external LDAP or RADIUS server.	<ul style="list-style-type: none"> <li>• <a href="#">External Authentication, page 5-11</a></li> </ul>
4.	(Optional) Create and order additional authentication realms.  Create at least one authentication realm for each authentication protocol and scheme combination you plan to use.	<ul style="list-style-type: none"> <li>• <a href="#">Creating Authentication Sequences, page 5-27</a></li> </ul>
5.	(Optional) Configure credential encryption.	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Credential Encryption, page 5-36</a></li> </ul>
6.	Create Identification Profiles to classify users and client software based on authentication requirements.	<ul style="list-style-type: none"> <li>• <a href="#">Classifying Users and Client Software, page 6-3</a></li> </ul>
7.	Create policies to manage Web requests from the users and user groups for which you created Identification Profiles.	<ul style="list-style-type: none"> <li>• <a href="#">Managing Web Requests Through Policies Best Practices, page 10-3</a></li> </ul>

## 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, page 5-29](#).

## Authentication Planning

- [Active Directory/Kerberos, page 5-3](#)
- [Active Directory/Basic, page 5-4](#)
- [Active Directory/NTLMSSP, page 5-5](#)
- [LDAP/Basic, page 5-5](#)
- [Identifying Users Transparently, page 5-5](#)

## Active Directory/Kerberos

Explicit Forward	Transparent, IP-Based Caching	Transparent, Cookie-Based Caching
<p><b>Advantages:</b></p> <ul style="list-style-type: none"> <li>• Better performance and interoperability when compared to NTLM</li> <li>• Works with both Windows and non-Windows clients that have joined the domain</li> <li>• Supported by all browsers and most other applications</li> <li>• RFC-based</li> <li>• Minimal overhead</li> <li>• Works for HTTPS (CONNECT) requests</li> <li>• Because the passphrase is not transmitted to the authentication server, it is more secure</li> <li>• Connection is authenticated, not the host or IP address</li> <li>• Achieves true single sign-on in an Active Directory environment when the client applications are configured to trust the Web Security appliance</li> </ul>	<p><b>Advantages:</b></p> <ul style="list-style-type: none"> <li>• Better performance and interoperability when compared to NTLM</li> <li>• Works with both Windows and non-Windows clients that have joined the domain</li> <li>• Works with all major browsers</li> <li>• With user agents that do not support authentication, users only need to authenticate first in a supported browser</li> <li>• Relatively low overhead</li> <li>• Works for HTTPS requests if the user has previously authenticated with an HTTP request</li> </ul>	<p><b>Advantages:</b></p> <ul style="list-style-type: none"> <li>• Better performance and interoperability when compared to NTLM</li> <li>• Works with both Windows and non-Windows clients that have joined the domain</li> <li>• Works with all major browsers</li> <li>• Authentication is associated with the user rather than the host or IP address</li> </ul> <p><b>Disadvantages:</b></p> <ul style="list-style-type: none"> <li>• Each new web domain requires the entire authentication process because cookies are domain specific</li> <li>• Requires cookies to be enabled</li> <li>• Does not work for HTTPS requests</li> </ul>

## Active Directory/Basic

Explicit Forward	Transparent, IP-Based Caching	Transparent, Cookie-Based Caching
<p><b>Advantages:</b></p> <ul style="list-style-type: none"> <li>Supported by all browsers and most other applications</li> <li>RFC-based</li> <li>Minimal overhead</li> <li>Works for HTTPS (CONNECT) requests</li> <li>Because the passphrase is not transmitted to the authentication server, it is more secure</li> <li>Connection is authenticated, not the host or IP address</li> <li>Achieves true single sign-on in an Active Directory environment when the client applications are configured to trust the Web Security appliance</li> </ul> <p><b>Disadvantages:</b></p> <ul style="list-style-type: none"> <li>Passphrase sent as clear text (Base64) for every request</li> <li>No single sign-on</li> <li>Moderate overhead: each new connection needs to be re-authenticated</li> <li>Primarily supported on Windows only and with major browsers only</li> </ul>	<p><b>Advantages:</b></p> <ul style="list-style-type: none"> <li>Works with all major browsers</li> <li>With user agents that do not support authentication, users only need to authenticate first in a supported browser</li> <li>Relatively low overhead</li> <li>Works for HTTPS requests if the user has previously authenticated with an HTTP request</li> </ul> <p><b>Disadvantages:</b></p> <ul style="list-style-type: none"> <li>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)</li> <li>No single sign-on</li> <li>Passphrase is sent as clear text (Base64)</li> </ul>	<p><b>Advantages:</b></p> <ul style="list-style-type: none"> <li>Works with all major browsers</li> <li>Authentication is associated with the user rather than the host or IP address</li> </ul> <p><b>Disadvantages:</b></p> <ul style="list-style-type: none"> <li>Each new web domain requires the entire authentication process because cookies are domain specific</li> <li>Requires cookies to be enabled</li> <li>Does not work for HTTPS requests</li> <li>No single sign-on</li> <li>Passphrase is sent as clear text (Base64)</li> </ul>

## Active Directory/NTLMSSP

Explicit Forward	Transparent
<p><b>Advantages:</b></p> <ul style="list-style-type: none"> <li>Because the passphrase is not transmitted to the authentication server, it is more secure</li> <li>Connection is authenticated, not the host or IP address</li> <li>Achieves true single sign-on in an Active Directory environment when the client applications are configured to trust the Web Security appliance</li> </ul> <p><b>Disadvantages:</b></p> <ul style="list-style-type: none"> <li>Moderate overhead: each new connection needs to be re-authenticated</li> <li>Primarily supported on Windows only and with major browsers only</li> </ul>	<p><b>Advantages:</b></p> <ul style="list-style-type: none"> <li>More Flexible</li> </ul> <p>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.</p> <p>The advantages and disadvantages of using transparent NTLM authentication are the same as those of using transparent Basic authentication except that <b>transparent NTLM authentication has the added advantage 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.</b></p>

## LDAP/Basic

Explicit Forward	Transparent
<p><b>Advantages:</b></p> <ul style="list-style-type: none"> <li>RFC-based</li> <li>More browser support than NTLM</li> <li>Minimal overhead</li> <li>Works for HTTPS (CONNECT) requests</li> </ul> <p><b>Disadvantages:</b></p> <ul style="list-style-type: none"> <li>No single sign-on</li> <li>Passphrase sent as clear text (Base64) for every request</li> </ul> <p><b>Workarounds:</b></p> <ul style="list-style-type: none"> <li><a href="#">Failed Authentication, page 5-28</a></li> </ul>	<p><b>Advantages:</b></p> <ul style="list-style-type: none"> <li>More Flexible than explicit forward.</li> <li>More browser support than NTLM</li> <li>With user agents that do not support authentication, users only need to authenticate first in a supported browser</li> <li>Relatively low overhead</li> <li>Works for HTTPS requests if the user has previously authenticated with an HTTP request</li> </ul> <p><b>Disadvantages:</b></p> <ul style="list-style-type: none"> <li>No single sign-on</li> <li>Passphrase is sent as clear text (Base64)</li> <li>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)</li> </ul> <p><b>Workarounds:</b></p> <ul style="list-style-type: none"> <li><a href="#">Failed Authentication, page 5-28</a></li> </ul>

## 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, page 5-33](#).

## Understanding Transparent User Identification

The available methods of transparent user identification are:

- **Transparently identify users with ISE** – Available when the Identity Services Engine (ISE) 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. See [Tasks for Certifying and Integrating the ISE Service, page 8-3](#).
- **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, page 10-20](#).
- **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, page 5-7](#).
  - **LDAP** – Create an LDAP authentication realm configured as an eDirectory, and enable transparent user identification. For more information, see [Transparent User Identification with LDAP, page 5-8](#).

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.

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 [Setting Up an Active Directory Agent to Provide Information to the Web Security Appliance, page 5-7](#).

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, page 5-9](#).
- 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 appliances.

### 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](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, page 5-9](#).
- 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 [Acquire End-User Credentials, page 5-1](#). 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](#), or the CLI command [sethostname](#).

## 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.

- [External Authentication, page 5-11](#)
- [Creating an Active Directory Realm for Kerberos Authentication Scheme, page 5-11](#)
- [How to Create an Active Directory Authentication Realm \(NTLMSSP and Basic\), page 5-14](#)
- [Creating an LDAP Authentication Realm, page 5-16](#)
- [About Deleting Authentication Realms, page 5-21](#)
- [Configuring Global Authentication Settings, page 5-21](#)

**Related Topics**

- [RADIUS User Authentication, page 12-8](#)
- [Authentication Sequences, page 5-26](#)

## 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, page 5-16](#)

---

**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, page 12-9](#).

## Creating an Active Directory Realm for Kerberos Authentication Scheme

**Before You Begin**

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

- Install Active Directory on one of these servers: Windows server 2003, 2008, 2008R2 or 2012.
  - Create a user on the Active Directory server that is a member of the Domain 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 7 and Mac OS 10.5+.
  - Use the kerbtray tool from the Windows Resource Kit to verify the Kerberos ticket on the client: <http://www.microsoft.com/en-us/download/details.aspx?id=17657>.
  - Ticket viewer application on Mac clients is available under main menu > KeyChain Access to view the Kerberos tickets.
- Ensure you have the rights and domain information needed to join the Web Security appliance to the Active Directory domain you wish to authenticate against.
  - Compare the current time on the Web Security appliance with the current time on the Active Directory server and verify that the difference is no greater than the time specified in the “Maximum tolerance for computer clock synchronization” option on the Active Directory server.
  - If the Web Security appliance is managed by a Security Management appliance, be prepared to ensure that same-named authentication realms on different Web Security appliances have identical properties defined on each appliance.
  - Web Security appliance configuration:
    - In explicit mode, the WSA host name (CLI command [sethostname](#)) and the proxy name configured in the browser must be the same.
    - In transparent mode, the WSA host name must be the same as the Redirect Hostname (see [Configuring Global Authentication Settings, page 5-21](#)). Further, the WSA host name and Redirect Hostname must be configured prior to creating a Kerberos realm.
  - Be aware that once you commit the new realm, you cannot change a realm’s authentication protocol.
  - Note that single sign on (SSO) must be configured on client browsers; see [Configuring Single-Sign-on, page 5-10](#).
  - To simplify use of logs, customize the access log to use the %m custom field parameter. See [Customizing Access Logs, page 11-26](#).

- 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:

- Configure the Active Directory Account:

Setting	Description
Active Directory Domain	The Active Directory serve3r domain name. Also known as a DNS Domain or realm.
NetBIOS domain name	If the network uses NetBIOS, provide the domain name. <b>Tip</b> If this option is not available use the <a href="#">setntlmsecuritymode</a> CLI command to verify that the NTLM security mode is set to “domain.”
Computer Account	Specify a location within the Active Directory domain where AsyncOS will create an Active Directory computer account, also known as a “machine trust account,” to uniquely identify the computer on the domain. If the Active Directory environment automatically deletes computer objects at particular intervals, specify a location for the computer account that is in a container, protected from automatic deletion.

- Click **Join Domain**.



**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 WSA. Affected clients will need to log off and log back in again.

- 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
<b>Enable Transparent User Identification using Active Directory agent</b>	Enter both the server name for the machine where the primary Context Directory agent is installed and the shared secret used to access it. (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. With this option selected, AsyncOS uses Transport Layer Security when communicating with the Active Directory server.

**Step 9** (Optional) Click **Start Test**. This will test the settings you have entered, ensuring they are correct before real users use them to authenticate. For details on the testing performed, see [•Create additional NTLM realms to authenticate users in domains that are not trusted by existing NTLM realms., page 5-21.](#)

**Step 10** Troubleshoot any issues found during testing.

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

---

#### What to Do Next

- Create an Identification Profile that uses the Kerberos authentication scheme. [Classifying Users and Client Software, page 6-3.](#)

## 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 appendix of this guide.
- Compare the current time on the Web Security appliance with the current time on the Active Directory server and verify that the difference is no greater than the time specified in the “Maximum tolerance for computer clock synchronization” option on the Active Directory server.
- If the Web Security appliance is managed by a Security Management appliance, be prepared to ensure that same-named authentication realms on different Web Security appliances have identical properties defined on each appliance.
- Be aware that once you commit the new realm, you cannot change a realm’s authentication protocol.
- The WSA 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 UDP)
  - 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, page 5-10.](#)

### 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)

**Step 1** Choose **Network > Authentication**.

**Step 2** Click **Add Realm**.

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

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

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

Example: `active.example.com`.

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

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

**Step 6** Join the appliance to the domain:

- Configure the Active Directory Account:

Setting	Description
Active Directory Domain	The Active Directory server domain name. Also known as a DNS Domain or realm.
NetBIOS domain name	If the network uses NetBIOS, provide the domain name.
Computer Account	Specify a location within the Active Directory domain where AsyncOS will create an Active Directory computer account, also known as a “machine trust account”, to uniquely identify the computer on the domain.  If the Active Directory environment automatically deletes computer objects at particular intervals, specify a location for the computer account that is in a container, protected from automatic deletion.

- Click **Join Domain**.



**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 WSA. Affected clients will need to log off and log back in again.

- 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.

- Click **Create Account**.

**Step 7** (Optional) Configure transparent authentication.

Setting	Description
<b>Enable Transparent User Identification using Active Directory agent</b>	Enter both the server name for the machine where the primary Context Directory agent is installed and the shared secret used to access it.  (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.  With this option selected, AsyncOS uses Transport Layer Security when communicating with the Active Directory server.

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

**Step 10** Submit and commit your changes.

## Creating an LDAP Authentication Realm

### Before You Begin

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

**Step 1** Choose **Network > Authentication**.

**Step 2** Click **Add Realm**.

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

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

**Step 5** Enter the LDAP authentication settings:

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

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

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

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

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

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

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

- Select **External Authentication Queries**.
- Identify the user accounts..

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

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

<b>Base DN</b>	The Base DN to navigate to the correct location in the LDAP directory tree to begin a search.
<b>Query String</b>	$(\&(\text{objectClass}=\text{posixAccount})(\text{uid}=\{\text{u}\}))$
<b>Attribute containing the user's full name</b>	<code>gecos</code>

- 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 [•Create additional NTLM realms to authenticate users in domains that are not trusted by existing NTLM realms., page 5-21](#).



**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. [Classifying Users and Client Software, page 6-3](#).

#### Related Topics

- [External Authentication, page 5-11](#)

## Using Multiple NTLM Realms and Domains

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

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

## About Deleting Authentication Realms

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

Deleting an authentication realm removes it from sequences.

## Configuring Global Authentication Settings

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

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

#### Before You Begin

- Be familiar with the following concepts:
  - [Failed Authentication, page 5-28](#)
  - [Failed Authorization: Allowing Re-Authentication with Different Credentials, page 5-33](#)

- 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	<p>Choose one of the following values:</p> <ul style="list-style-type: none"> <li>• <b>Permit traffic to proceed without authentication.</b> Processing continues as if the user was authenticated.</li> <li>• <b>Block all traffic if user authentication fails.</b> Processing is discontinued and all traffic is blocked.</li> </ul>
Failed Authentication Handling	<p>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.</p> <p>For more information on granting users guest access, see <a href="#">Granting Guest Access After Failed Authentication, page 5-31</a>.</p>
Re-authentication (Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction)	<p>This setting allows users to authenticate again if the user is blocked from a website due to a restrictive URL filtering policy or due to being restricted from logging into another IP address.</p> <p>The user sees a block page that includes a link that allows them to enter new authentication credentials. If the user enters credentials that allow greater access, the requested page appears in the browser.</p> <p><b>Note:</b> This setting only applies to authenticated users who are blocked due to restrictive URL filtering policies or User Session Restrictions. It does not apply to blocked transactions by subnet with no authentication.</p> <p>For more information, see <a href="#">Failed Authorization: Allowing Re-Authentication with Different Credentials, page 5-33</a>.</p>
Basic Authentication Token TTL	<p>Controls the length of time that user credentials are stored in the cache before revalidating them with the authentication server. This includes the username and passphrase and the directory groups associated with the user.</p> <p>The default value is the recommended setting. When the Surrogate Timeout setting is configured and is greater than the Basic Authentication Token TTL, then the Surrogate Timeout value takes precedence and the Web Proxy contacts the authentication server after surrogate timeout expires.</p>

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

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

Setting	Description
Credential Encryption	<p>This setting specifies whether or not the client sends the login credentials to the Web Proxy through an encrypted HTTPS connection.</p> <p>This setting applies to both Basic and NTLMSSP authentication schemes, but it is particularly useful for Basic authentication scheme because user credentials are sent as plain text.</p> <p>For more information, see <a href="#">Failed Authentication, page 5-28</a>.</p>
HTTPS Redirect Port	<p>Specify a TCP port to use for redirecting requests for authenticating users over an HTTPS connection.</p> <p>This specifies through which port the client will open a connection to the Web Proxy using HTTPS. This occurs when credential encryption is enabled or when using Access Control and users are prompted to authenticate.</p>
Redirect Hostname	<p>Enter the short hostname of the network interface on which the Web Proxy listens for incoming connections.</p> <p>When you configure authentication on an appliance deployed in transparent mode, the Web Proxy uses this hostname in the redirection URL sent to clients for authenticating users.</p> <p>You can enter either the following values:</p> <ul style="list-style-type: none"> <li><b>Single word hostname.</b> 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 <code>mycompany.com</code> and the interface on which the Web Proxy is listening has a full hostname of <code>proxy.mycompany.com</code>, then you should enter <code>proxy</code> in this field. Clients perform a lookup on <code>proxy</code> and they should be able to resolve <code>proxy.mycompany.com</code>.</li> <li><b>Fully qualified domain name (FQDN).</b> 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.</li> </ul>
Credential Cache Options: Surrogate Timeout	<p>This setting specifies how long the Web Proxy waits before asking the client for authentication credentials again. Until the Web Proxy asks for credentials again, it uses the value stored in the surrogate (IP address or cookie).</p> <p>It is common for user agents, such as browsers, to cache the authentication credentials so the user will not be prompted to enter credentials each time.</p>

Setting	Description
Credential Cache Options: Client IP Idle Timeout	<p>When IP address is used as the authentication surrogate, this setting specifies how long the Web Proxy waits before asking the client for authentication credentials again when the client has been idle.</p> <p>When this value is greater than the Surrogate Timeout value, this setting has no effect and clients are prompted for authentication after the Surrogate Timeout is reached.</p> <p>You might want to use this setting to reduce the vulnerability of users who leave their computers.</p>
Credential Cache Options: Cache Size	<p>Specifies the number of entries that are stored in the authentication cache. Set this value to safely accommodate the number of users that are actually using this device. The default value is the recommended setting.</p>
User Session Restrictions	<p>This setting specifies whether or not authenticated users are allowed to access the Internet from multiple IP addresses simultaneously.</p> <p>You might want to restrict access to one machine to prevent users from sharing their authentication credentials with non-authorized users. When a user is prevented from logging in at a different machine, an end-user notification page appears. You can choose whether or not users can click a button to login as a different username using the Re-authentication setting on this page.</p> <p>When you enable this setting, enter the restriction timeout value, which determines how long users must wait before being able to log into a machine with a different IP address. The restriction timeout value must be greater than the surrogate timeout value.</p> <p>You can remove a specific user or all users from the authentication cache using the <code>authcache</code> CLI command.</p>
Advanced	<p>When using Credential Encryption or Access Control, you can choose whether the appliance uses the digital certificate and key shipped with the appliance (the Cisco Web Security Appliance Demo Certificate) or a digital certificate and key you upload here.</p>

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

Setting	Description
Credential Encryption	<p>This setting specifies whether or not the client sends the login credentials to the Web Proxy through an encrypted HTTPS connection. To enable credential encryption, choose “HTTPS Redirect (Secure)”. When you enable credential encryption, additional fields appear to configure how to redirect clients to the Web Proxy for authentication.</p> <p>This setting applies to both Basic and NTLMSSP authentication schemes, but it is particularly useful for Basic authentication scheme because user credentials are sent as plain text.</p> <p>For more information, see <a href="#">Failed Authentication, page 5-28</a>.</p>
HTTPS Redirect Port	<p>Specify a TCP port to use for redirecting requests for authenticating users over an HTTPS connection.</p> <p>This specifies through which port the client will open a connection to the Web Proxy using HTTPS. This occurs when credential encryption is enabled or when using Access Control and users are prompted to authenticate.</p>
Redirect Hostname	<p>Enter the short host name of the network interface on which the Web Proxy listens for incoming connections.</p> <p>When you enable Authentication Mode above, the Web Proxy uses this hostname in the redirection URL sent to clients for authenticating users.</p> <p>You can enter either the following values:</p> <ul style="list-style-type: none"> <li><b>Single word hostname.</b> 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 <code>mycompany.com</code> and the interface on which the Web Proxy is listening has a full host name of <code>proxy.mycompany.com</code>, then you should enter <code>proxy</code> in this field. Clients perform a lookup on <code>proxy</code> and they should be able to resolve <code>proxy.mycompany.com</code>.</li> <li><b>Fully qualified domain name (FQDN).</b> 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.</li> </ul>
Credential Cache Options: Surrogate Timeout	<p>This setting specifies how long the Web Proxy waits before asking the client for authentication credentials again. Until the Web Proxy asks for credentials again, it uses the value stored in the surrogate (IP address or cookie).</p> <p>Note that it is common for user agents, such as browsers, to cache the authentication credentials so the user will not be prompted to enter credentials each time.</p>

Setting	Description
Credential Cache Options: Client IP Idle Timeout	<p>When IP address is used as the authentication surrogate, this setting specifies how long the Web Proxy waits before asking the client for authentication credentials again when the client has been idle.</p> <p>When this value is greater than the Surrogate Timeout value, this setting has no effect and clients are prompted for authentication after the Surrogate Timeout is reached.</p> <p>You might want to use this setting to reduce the vulnerability of users who leave their computers.</p>
Credential Cache Options: Cache Size	<p>Specifies the number of entries that are stored in the authentication cache. Set this value to safely accommodate the number of users that are actually using this device. The default value is the recommended setting.</p>
User Session Restrictions	<p>This setting specifies whether or not authenticated users are allowed to access the Internet from multiple IP addresses simultaneously.</p> <p>You might want to restrict access to one machine to prevent users from sharing their authentication credentials with non-authorized users. When a user is prevented from logging at a different machine, an end-user notification page appears. You can choose whether or not users can click a button to login as a different username using the Re-authentication setting on this page.</p> <p>When you enable this setting, enter the restriction timeout value, which determines how long users must wait before being able to log into a machine with a different IP address. The restriction timeout value must be greater than the surrogate timeout value.</p> <p>You can remove a specific user or all users from the authentication cache using the <code>authcache</code> CLI command.</p>
Advanced	<p>When using Credential Encryption or Access Control, you can choose whether the appliance uses the digital certificate and key shipped with the appliance (the Cisco Web Security Appliance Demo Certificate) or a digital certificate and key you upload here.</p> <p>To upload a digital certificate and key, click <b>Browse</b> and navigate to the necessary file on your local machine. Then click <b>Upload Files</b> after you select the files you want.</p>

- Step 6** Submit and commit your changes.

## Authentication Sequences

- [About Authentication Sequences, page 5-27](#)
- [Creating Authentication Sequences, page 5-27](#)
- [Editing And Reordering Authentication Sequences, page 5-28](#)
- [Editing And Reordering Authentication Sequences, page 5-28](#)

## About Authentication Sequences

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

Authentication sequences are collections of two or more authentication realms. The realms used can have different authentication servers and different authentication protocols. For more information on authentication realms, see [Authentication Realms, page 5-10](#).

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

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

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

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

**Tip**

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

## Creating Authentication Sequences

### Before You Begin

- Create two or more authentication realms (see [Authentication Realms, page 5-10](#)).
- If the Web Security appliance is managed by a Security Management appliance, ensure that same-named authentication realms on different Web Security appliances have identical properties defined on each appliance.
- Be aware that AsyncOS will use the realms to process authentication sequentially, beginning with the first realm in the list.

---

**Step 1** Choose **Network > Authentication**

**Step 2** Click **Add Sequence**.

**Step 3** Enter a unique name for the sequence using alphanumeric and space characters.

**Step 4** In the first row of the Realm Sequence for Basic Scheme area, choose the first authentication realm you want to include in the sequence.

**Step 5** In the second row of the Realm Sequence for Basic Scheme area, choose the next realm you want to include in the sequence.

**Step 6** (Optional) Click **Add Row** to include another realm that uses Basic credentials.

**Failed Authentication**

- Step 7** If an NTLM realm is defined, choose an NTLM realm in the Realm for NTLMSSP Scheme field. The Web Proxy uses this NTLM realm when the client sends NTLMSSP authentication credentials.
- Step 8** Submit and commit your changes.
- 

## Editing And Reordering Authentication Sequences

- Step 1** Choose **Network > Authentication**.
- Step 2** Click the name of the sequence you wish to edit or re-order.
- Step 3** Choose a realm name from the Realms drop-down list on the row corresponding to the position number you want the realm to occupy in the sequence.
-  **Note** For the All Realms sequence, you can only change the order of its realms, you cannot change the realms themselves. To change the order of realms in the All Realms sequence, click the arrows in the Order column to reposition the corresponding realms.
- 
- Step 4** Repeat Step 3 until all realms are listed and ordered as required, ensuring that each realm name appears in one row only.
- Step 5** Submit and commit your changes.
- 

## Deleting Authentication Sequences

### Before You Begin

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

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

## Failed Authentication

- [About Failed Authentication, page 5-29](#)
- [Bypassing Authentication with Problematic User Agents, page 5-29](#)
- [Bypassing Authentication, page 5-31](#)
- [Permitting Unauthenticated Traffic While Authentication Service is Unavailable, page 5-31](#)

- [Granting Guest Access After Failed Authentication, page 5-31](#)
- [Failed Authorization: Allowing Re-Authentication with Different Credentials, page 5-33](#)

## 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, page 5-29](#)
- [Bypassing Authentication, page 5-31](#)
- [Permitting Unauthenticated Traffic While Authentication Service is Unavailable, page 5-31](#)
- [Granting Guest Access After Failed Authentication, page 5-31](#)

## 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.

- 
- Step 1** Configure the Identification Profile to bypass authentication with the specified user agents:
- Select **Web Security Manager > Identification Profile**.
  - Click **Add Identification Profile**.
  - 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.

- Click **Advanced > User Agents**.
- Click **None Selected**.
- Under Custom user Agents, specify the problematic User Agent strings.

- Step 2** Configure the Access Policy:

- Choose **Web Security Manager > Access Policies**.
- Click **Add Policy**.
- 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.	<a href="#">Creating and Editing Custom URL Categories, page 9-14</a>
2. Create an Identification Profile with these characteristics: <ul style="list-style-type: none"> <li data-bbox="447 523 829 587">– Placed above all identities that require authentication.</li> <li data-bbox="447 595 878 637">– Includes the custom URL category.</li> <li data-bbox="447 646 894 688">– Includes affected client applications.</li> <li data-bbox="447 696 838 718">– Does not require authentication</li> </ul>	<a href="#">Classifying Users and Client Software, page 6-3</a>
3. Create a policy for the Identification Profile.	<a href="#">Creating a Policy, page 10-7</a>

### Related Topics

- Bypassing the Web Proxy

## Permitting Unauthenticated Traffic While Authentication Service is Unavailable


**Note**

This configuration applies only when an authentication service is unavailable. It will not bypass authentication permanently. For alternative options, see [About Failed Authentication, page 5-29](#)

**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, page 5-32](#)
2. [Use an Identification Profile that Supports Guest Access in a Policy, page 5-32](#)
3. (Optional) [Configure How Guest User Details are Logged, page 5-32](#)


**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

**Failed Authentication**

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

- 
- 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

- 
- 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.



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, page 5-32](#) to define a new one.

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

## Configure How Guest User Details are Logged

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

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

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

## Failed Authorization: Allowing Re-Authentication with Different Credentials

- [About Allowing Re-Authentication with Different Credentials, page 5-33](#)
- [Allowing Re-Authentication with Different Credentials, page 5-33](#)

### About Allowing Re-Authentication with Different Credentials

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

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

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

### Allowing Re-Authentication with Different Credentials

---

**Step 1** Choose **Network > Authentication**.

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

**Step 3** Check the **Re-Authentication Prompt If End User Blocked by URL Category Or User Session Restriction** check box.

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

---

## Tracking Identified Users



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

---

## 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, page 6-3](#).

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, page 6-7](#)

## 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, page 5-35](#)
- [Authentication and Authorization Failures, page 5-36](#)
- [Credential Format, page 5-36](#)
- [Credential Encryption for Basic Authentication, page 5-36](#)

## 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](#), 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, page 5-31](#)
- [Allowing Re-Authentication with Different Credentials, page 5-33](#)

## Credential Format

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

## Credential Encryption for Basic Authentication

### About Credential Encryption for Basic Authentication

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

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

## Configuring Credential Encryption

### Before You Begin:

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

---

**Step 1** Choose Network > Authentication.

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

**Step 3** Check the **Use Encrypted HTTPS Connection For Authentication** check box in the Credential Encryption field.

- Step 4** (Optional) Edit the default port number (443) in the HTTPS Redirect Port field for client HTTP connections during authentication.
- Step 5** (Optional) Upload a certificate and key:
- Expand the Advanced section.
  - Click **Browse** in the Certificate field and find the certificate file you wish to upload.
  - Click **Browse** in the Key field and find the private key file you wish to upload.
  - Click **Upload Files**.
- Step 6** Submit and commit your changes.
- 

#### Related Topics

- [Certificate Management, page 12-24.](#)

## Troubleshooting Authentication

- [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication, page A-10](#)
- [Cannot Access URLs that Do Not Support Authentication, page A-13](#)
- [Client Requests Fail Upstream Proxy, page A-14](#)





## Classify End-Users and Client Software

---

- [Overview of Classify Users and Client Software, page 6-1](#)
- [Classify Users and Client Software: Best Practices, page 6-2](#)
- [Identification Profile Criteria, page 6-2](#)
- [Classifying Users and Client Software, page 6-3](#)
- [Identification Profiles and Authentication, page 6-7](#)
- [Troubleshooting Identification Profiles, page 6-8](#)

### 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

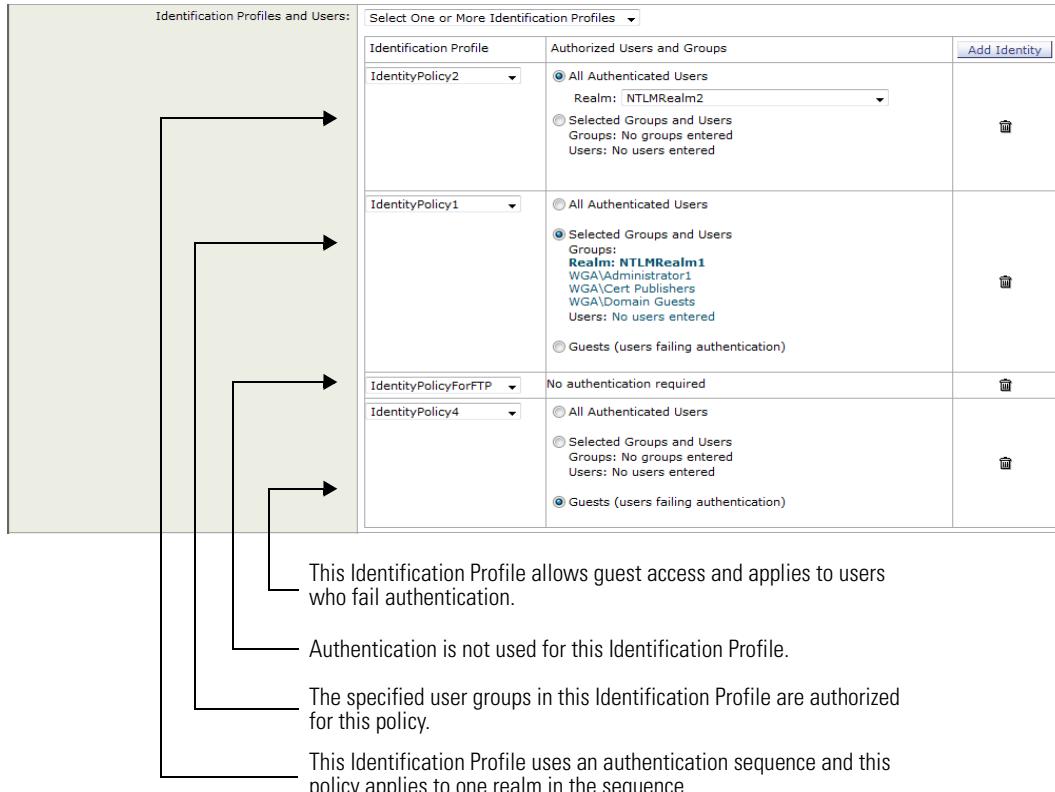
AsyncOS assigns an Identification Profile to every transaction:

- 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:



## 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](#), page 5-31.

## 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 \(NTLMSSP and Basic\), page 5-14](#) or [Creating an LDAP Authentication Realm, page 5-16](#).
- 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, page 3-7](#).
- (Optional) Create authentication sequences. See [Creating Authentication Sequences, page 5-27](#)
- (Optional) Enable Secure Mobility if the Identification Profile will include mobile users.
- (Optional) Understand authentication surrogates. See [Tracking Identified Users, page 5-33](#).

**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.

There are two types of methods: exempt from authentication/identification and authenticate users.

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

Option	Description
<b>Exempt from authentication/identification</b>	Users are identified primarily by IP address. No additional parameters are required.
<b>Authenticate users</b>	Users are identified by the authentication credentials they enter.



- 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.

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

<b>Authentication Realm</b>	<p><b>Select a Realm or Sequence</b> – choose a defined authentication realm or sequence.</p> <p><b>Select a Scheme</b> – Choose an authentication scheme:</p> <ul style="list-style-type: none"> <li>• <b>Kerberos</b> – The client is transparently authenticated by means of Kerberos tickets.</li> <li>• <b>Basic</b> – 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.</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>• <b>NTLMSSP</b> – The client transparently authenticates using its Windows login credentials. The user is not prompted for credentials. However, the client prompts the user for credentials under the following circumstances:           <ul style="list-style-type: none"> <li>– The Windows credentials failed.</li> <li>– The client does not trust the Web Security appliance because of browser security settings.</li> </ul> </li> </ul> <p>Credentials are sent securely using a three-way handshake (digest style authentication). The passphrase is never sent across the connection.</p> <ul style="list-style-type: none"> <li>• <b>Support Guest privileges</b> – Check this box to grant guest access to users who fail authentication due to invalid credentials.</li> </ul>
-----------------------------	--

<b>Authentication Surrogates</b>	<p>Specify how transactions will be associated with a user after successful authentication (options vary depending on Web Proxy deployment mode):</p> <ul style="list-style-type: none"> <li>• <b>IP Address</b> – The Web Proxy tracks an authenticated user at a particular IP address. For transparent user identification, select this option.</li> <li>• <b>Persistent Cookie</b> – 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.</li> <li>• <b>Session Cookie</b> – 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.</li> <li>• <b>Apply same surrogate settings to explicit forward requests</b> – 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.</li> </ul> <p><b>Note</b> You can define a timeout value for the authentication surrogate for all requests in Global Authentication Settings.</p>
----------------------------------	---

- 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.

<b>Membership Definition</b>	
<b>Define Members by Subnet</b>	<p>Enter the addresses to which this Identification Profile should apply. You can use IP addresses, CIDR blocks, and subnets.</p> <p><b>Note</b> If nothing is entered, the Identification Profile applies to <i>all</i> IP addresses.</p>

---

<b>Advanced</b>	Expand this section to define additional membership requirements.
	<ul style="list-style-type: none"> <li>• <b>Proxy Ports</b> – 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. For transparent connections, this is the same as the destination port. 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.</li> <li>• <b>URL Categories</b> – 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. 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.</li> <li>• <b>User Agents</b> – 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. 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</li> </ul>

---

**Step 9 Submit and Commit Changes.****Related Topics**

- [Overview of Acquire End-User Credentials, page 5-1](#)
- [Managing Web Requests Through Policies Task Overview, page 10-3](#)

## 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.

**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.

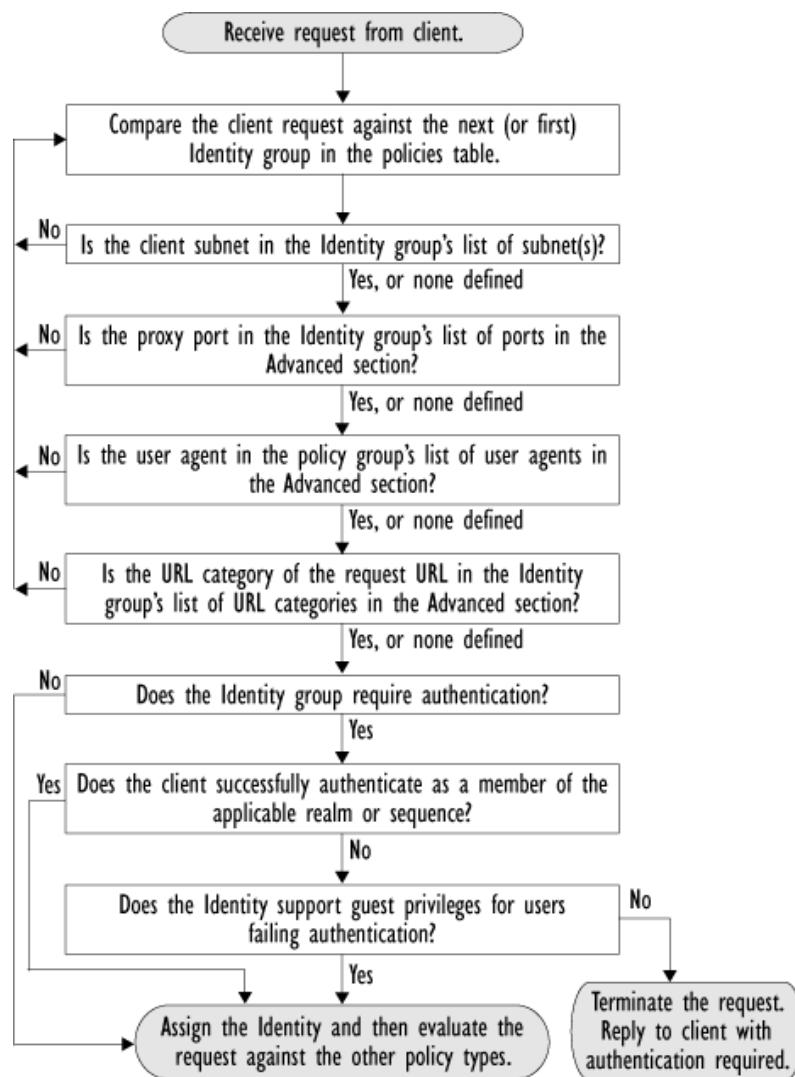
**Step 4 Submit and Commit Changes.**

# 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:

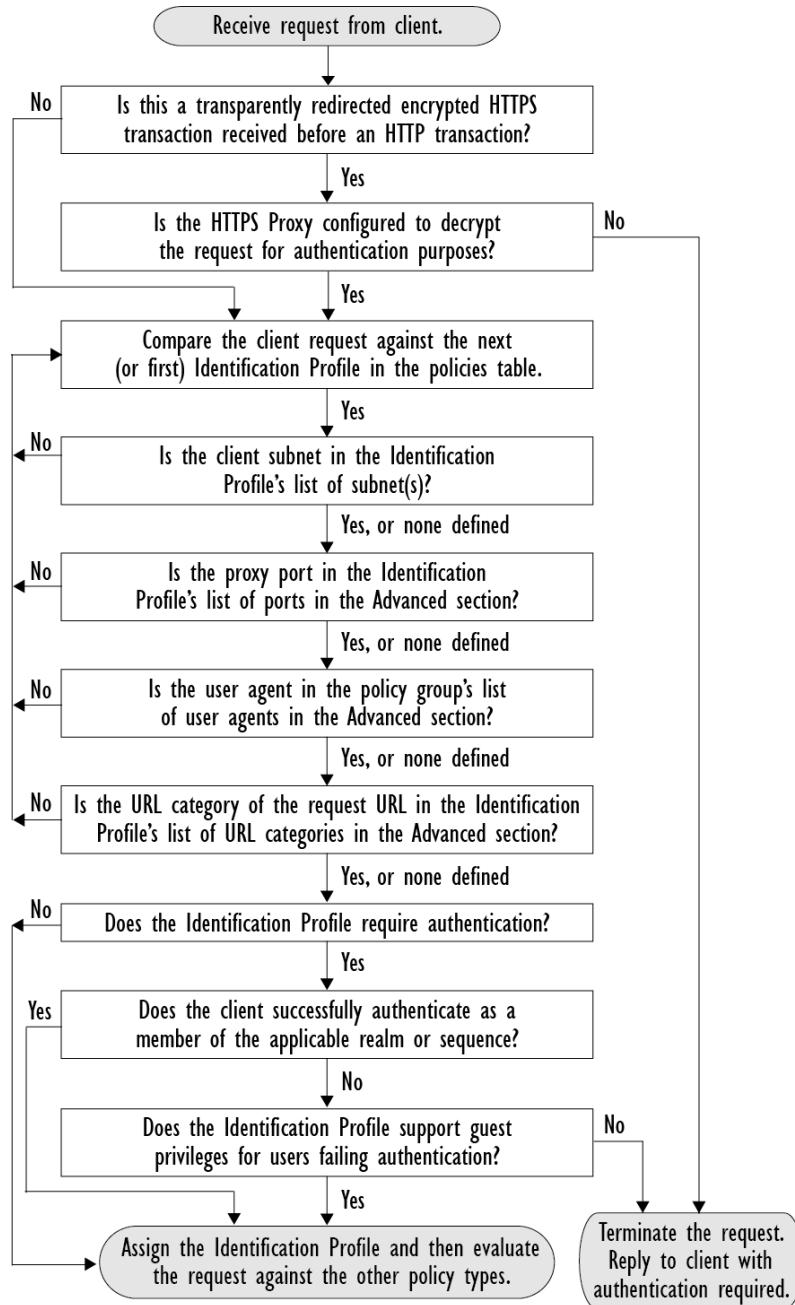
- No authentication surrogates
- IP addresses as authentication surrogates
- Cookies as authentication surrogates with transparent requests
- Cookies as authentication surrogates with explicit requests and credential encryption is enabled

**Figure 6-1 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 6-2 Identification Profiles and Authentication Processing – Cookie-based Surrogates**



## Troubleshooting Identification Profiles

- Policy Problems, page A-9

- Policy is Never Applied, page A-10
- Upstream Proxy Problems, page A-14

**Troubleshooting Identification Profiles**



# Create Decryption Policies to Control HTTPS Traffic

---

- [Overview of Create Decryption Policies to Control HTTPS Traffic, page 7-1](#)
- [Managing HTTPS Traffic through Decryption Policies Best Practices, page 7-2](#)
- [Decryption Policies, page 7-2](#)
- [Root Certificates, page 7-7](#)
- [Routing HTTPS Traffic, page 7-13](#)

## 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	<a href="#">Enabling the HTTPS Proxy, page 7-3</a>
2	Upload or Generate a certificate and key	<ul style="list-style-type: none"> <li><a href="#">Uploading a Root Certificate and Key, page 7-9</a></li> <li><a href="#">Generating a Certificate and Key for the HTTPS Proxy, page 7-10</a></li> </ul>
3	Configuring Decryption options	<a href="#">Configuring Decryption Options, page 7-7</a>
5	(Optional) Configure invalid certificate handling	<a href="#">Configuring Invalid Certificate Handling, page 7-10</a>
6	(Optional) Enabling real-time revocation status checking	<a href="#">Enabling Real-Time Revocation Status Checking, page 7-12</a>
7	(Optional) Manage trusted and blocked certificates	<a href="#">Trusted Root Certificates, page 7-12</a>

## Managing HTTPS Traffic through Decryption Policies Best Practices

- Create fewer, more general Decryption Policy groups that apply to all users or fewer, larger groups of users on the network. Then, if you need to apply more granular control to decrypted HTTPS traffic, use more specific Access Policy groups.

## Decryption Policies

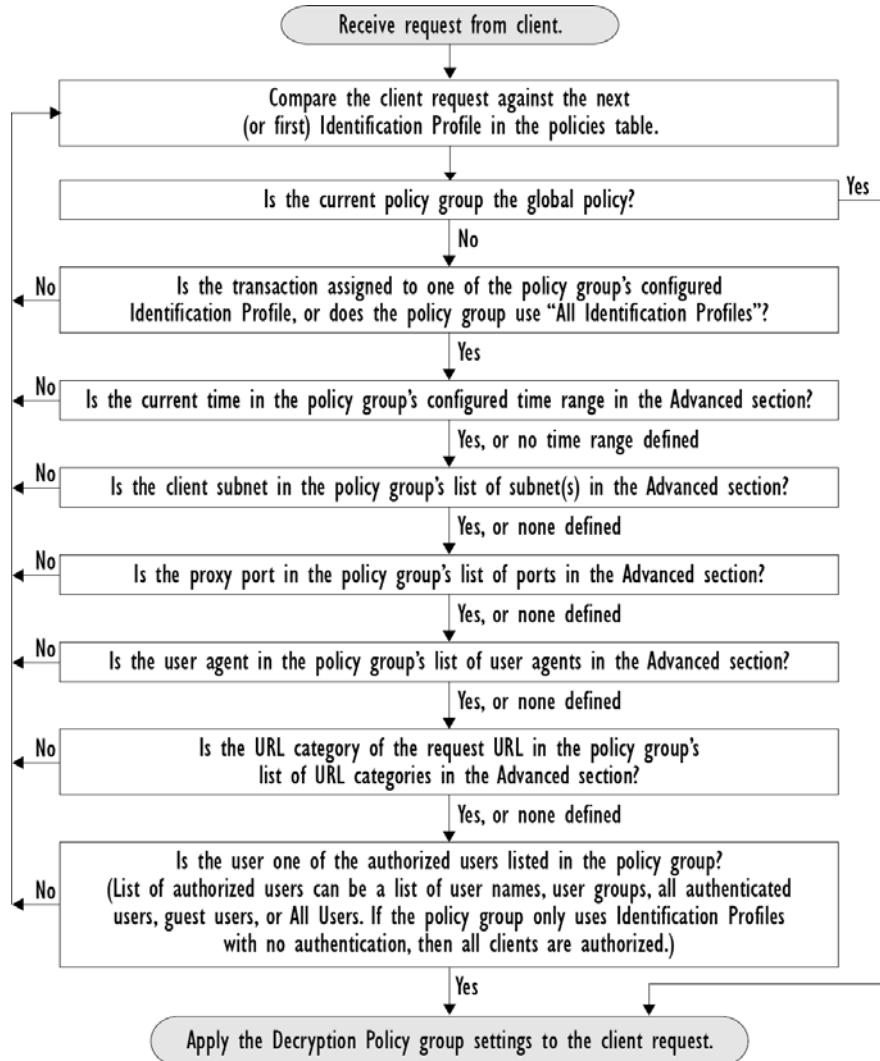
The appliance can perform any of the following actions on an HTTPS connection request:

Option	Description
Monitor	Monitor is an intermediary action that indicates the Web Proxy should continue evaluating the transaction against the other control settings to determine which final action to ultimately apply.
Drop	The appliance drops the connection and does not pass the connection request to the server. The appliance does not notify the user that it dropped the connection.
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. [Figure 7-2 on page 7-6](#) shows the order the Web Proxy uses when evaluating control settings for Decryption Policies. [Figure 10-3 on page 10-13](#) shows the order the Web Proxy uses when evaluating control settings for Access Policies.

**Figure 7-1 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.

**Step 1** Security Services > HTTPS Proxy, click **Enable and Edit Settings**.

The HTTPS Proxy License Agreement appears.

**Step 2** Read the terms of the HTTPS Proxy License Agreement, and click **Accept**.

**Step 3** Verify the Enable HTTPS Proxy field is enabled.

**Step 4** In the HTTPS Ports to Proxy field, enter the ports the appliance should check for HTTPS traffic. Port 443 is the default port.



**Note** The maximum number of ports for which the Web Security appliance can serve as proxy is 30, which includes both HTTP and HTTPS.

**Step 5** Upload or generate a root/signing certificate to use for decryption.



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

**Step 6** In the HTTPS Transparent Request section, select one of the following options:

- Decrypt the HTTPS request and redirect for authentication
- Deny the HTTPS request

This setting only applies to transactions that use IP address as the authentication surrogate and when the user has not yet been authenticated.



**Note** This field only appears when the appliance is deployed in transparent mode.

**Step 7** In the Applications that Use HTTPS section, choose whether to enable decryption for enhanced application visibility and control.



**Note** Decryption may cause some applications to fail unless the root certificate for signing is installed on the client. For more information on the appliance root certificate, see.

**Step 8** Submit and commit your changes.

**Related Topics**

- [Managing Certificate Validation and Decryption for HTTPS, page 7-8](#)

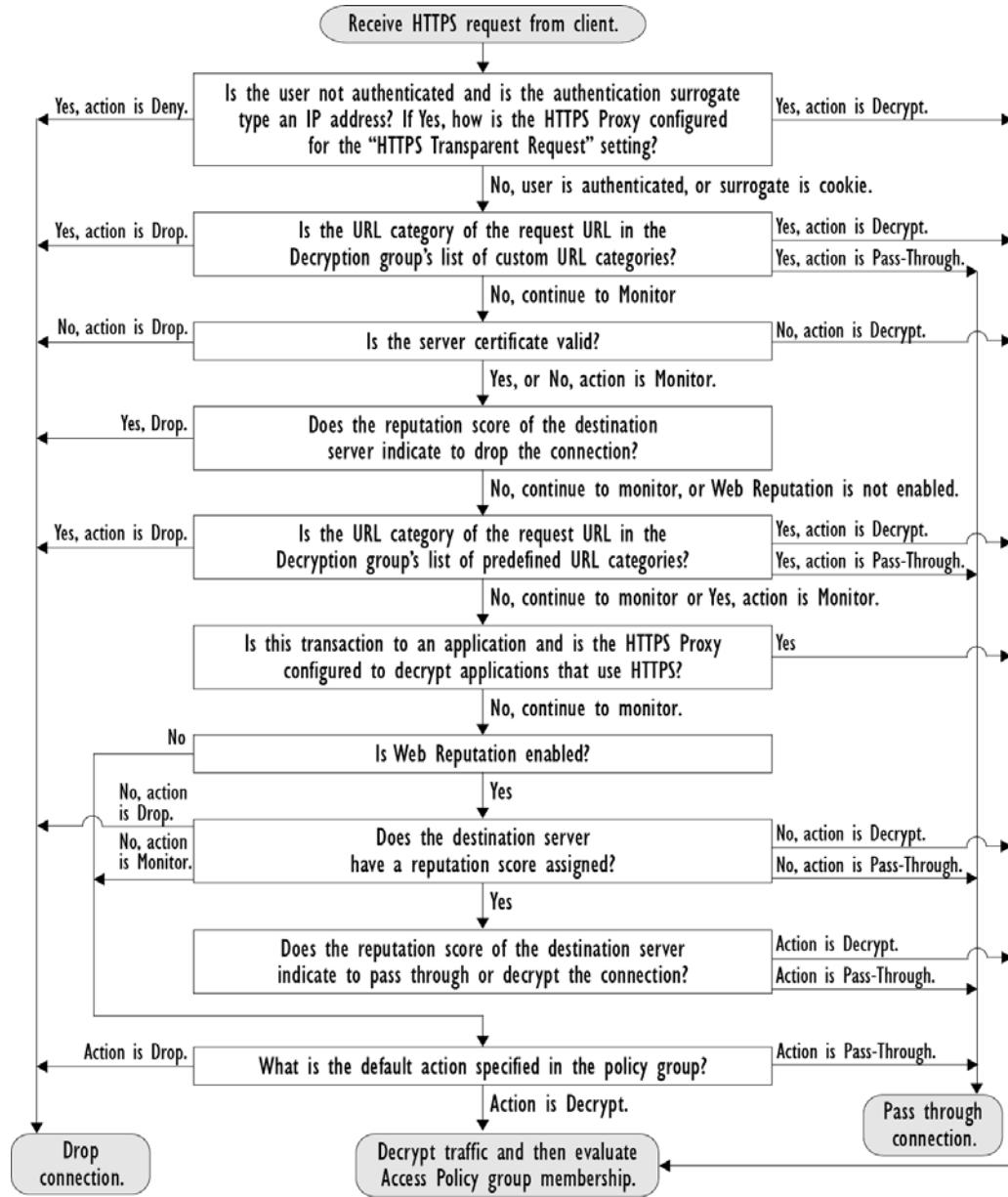
## Controlling HTTPS Traffic

After the Web Security appliance assigns an HTTPS connection request to a Decryption Policy group, the connection request inherits the control settings of that policy group. The control settings of the Decryption Policy group determine whether the appliance decrypts, drops, or passes through the connection:

Option	Description
URL Categories	<p>You can configure the action to take on HTTPS requests for each predefined and custom URL category. Click the link under the URL Filtering column for the policy group you want to configure.</p> <p><b>Note</b> If you want to <i>block</i> (with end-user notification) a particular URL category for HTTPS requests instead of drop (with no end-user notification), choose to decrypt that URL category in the Decryption Policy group and then choose to block the same URL category in the Access Policy group.</p>
Web Reputation	<p>You can configure the action to take on HTTPS requests based on the web reputation score of the requested server. Click the link under the Web Reputation column for the policy group you want to configure.</p>
Default Action	<p>You can configure the action the appliance should take when none of the other settings apply. Click the link under the Default Action column for the policy group you want to configure.</p> <p><b>Note</b> The configured default action only affects the transaction when no decision is made based on URL category or Web Reputation score. If Web Reputation filtering is disabled, the default action applies to all transactions that match a Monitor action in a URL category. If Web Reputation filtering is enabled, the default action is used only if the Monitor action is selected for sites with no score.</p>

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 7-2 Applying Decryption Policy Actions**



## Configuring Decryption Options

### Before You Begin

- Verify that the HTTPS proxy is enabled as described in [Enabling the HTTPS Proxy, page 7-3](#)

**Step 1** Security Services > HTTPS Proxy.

**Step 2** Click Edit Settings.

**Step 3** Enable the decryption options.

Decryption Option	Description
Decrypt for Authentication	For users who have not been authenticated prior to this HTTPS transaction, allow decryption for authentication.
Decrypt for End-User Notification	Allow decryption so that AsyncOS can display the end-user notification. <b>Note</b> 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	<ul style="list-style-type: none"> <li>secure client authentication disabled or</li> <li>secure client authentication enabled and an IP-based surrogate</li> </ul>
Transparent requests	<ul style="list-style-type: none"> <li>IP-based surrogate, decryption for authentication enabled or</li> <li>IP-based surrogate, client previously authenticated using an HTTP request</li> </ul>

## 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, page 12-24](#) 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.

---

**Step 1** Security Services > HTTPS Proxy.

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

**Step 3** Click the Download Certificate link for either the generated or uploaded certificate.

**Note**

To reduce the possibility of client machines getting a certificate error, submit the changes after you generate or upload the root certificate to the Web Security appliance, then distribute the certificate to client machines, and then commit the changes to the appliance.

## Managing Certificate Validation and Decryption for HTTPS

The Web Security appliance validates certificates before inspecting and decrypting content.

### Valid Certificates

Qualities of a valid certificate:

- **Not expired.** The certificate's validity period includes the current date.
- **Recognized certificate authority.** The issuing certificate authority is included in the list of trusted certificate authorities stored on the Web Security appliance.
- **Valid signature.** The digital signature was properly implemented based on cryptographic standards.
- **Consistent naming.** The common name matches the hostname specified in the HTTP header.
- **Not revoked.** The issuing certificate authority has not revoked the certificate.

#### Related Topics

- [Managing Certificate Validation and Decryption for HTTPS, page 7-8](#)
- [Configuring Invalid Certificate Handling, page 7-10](#)

- Options for Certificate Revocation Status Checking, page 7-11
- Enabling Real-Time Revocation Status Checking, page 7-12

## Invalid Certificate Handling

The appliance can perform one of the following actions for invalid server certificates:

- **Drop.**
- **Decrypt.**
- **Monitor.**

### Certificates that are Invalid for Multiple Reasons

For server certificates that are invalid due to both an unrecognized root authority and an expired certificate, the HTTPS proxy performs the action that applies to unrecognized root authorities.

In all other cases, for server certificates that are invalid for multiple reasons simultaneously, the HTTPS Proxy performs actions in order from the most restrictive action to the least restrictive action.

### Untrusted Certificate Warnings for Decrypted Connections

When the Web Security appliance encounters an invalid certificate and is configured to decrypt the connection, AsyncOS creates an untrusted certificate that requires the end-user to accept or reject the connection. The common name of the certificate is “Untrusted Certificate Warning.”

Adding this untrusted certificate to the list of trusted certificates will remove the end user’s option to accept or reject the connection.

When AsyncOS generates one of these certificates, it creates a proxy log entry with the text “Signing untrusted key” or “Signing untrusted cert”.

## Uploading a Root Certificate and Key

### Before You Begin

- Enable the HTTPS Proxy. [Enabling the HTTPS Proxy, page 7-3](#).

---

**Step 1** **Security Services > HTTPS Proxy.**

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

**Step 3** Select **Use Uploaded Certificate and Key**.

**Step 4** Click **Browse** for the **Certificate** field to navigate to the certificate file stored on the local machine.

If the file you upload contains multiple certificates or keys, the Web Proxy uses the first certificate or key in the file.

**Step 5** Click **Browse** for the **Key** field to navigate to the private key file.



---

**Note** The key length must be 512, 1024, or 2048 bits.

---

**Step 6** Select **Key is Encrypted** if the key is encrypted.

**Step 7** Click **Upload Files** to transfer the certificate and key files to the Web Security appliance.

The uploaded certificate information is displayed on the Edit HTTPS Proxy Settings page.

- Step 8** (Optional) Click **Download Certificate** so you can transfer it to the client applications on the network.
- 

## Generating a Certificate and Key for the HTTPS Proxy

### Before You Begin

- Enable the HTTPS Proxy. [Enabling the HTTPS Proxy, page 7-3](#).

- 
- Step 1** **Security Services > HTTPS Proxy.**

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

- Step 3** Select **Use Generated Certificate and Key**.

- Step 4** Click **Generate New Certificate and Key**.

- Step 5** In the Generate Certificate and Key dialog box, enter the information to display in the root certificate.

You can enter any ASCII character except the forward slash ( / ) in the **Common Name** field.

- Step 6** Click **Generate**.

- Step 7** The generated certificate information is displayed on the Edit HTTPS Proxy Settings page.

- Step 8** (Optional) Click **Download Certificate** so you can transfer it to the client applications on the network.

- Step 9** (Optional) Click the **Download Certificate Signing Request** link. so you can submit the Certificate Signing Request (CSR) to a certificate authority (CA).

- Step 10** (Optional) Upload the signed certificate to the Web Security appliance after receiving it back from the CA. You can do this at anytime after generating the certificate on the appliance.

- Step 11** **Submit and Commit Changes.**
- 

## Configuring Invalid Certificate Handling

### Before You Begin

- Verify that the HTTPS proxy is enabled as described in [Enabling the HTTPS Proxy, page 7-3](#)

- 
- Step 1** **Security Services > HTTPS Proxy.**

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

**Step 3** For each type of certificate error, define the proxy response, **Drop**, **Decrypt** or **Monitor**.

Certificate Error Type	Description
Expired	The current date falls outside of the range of validity for the certificate.
Mismatched hostname	The hostname in the certificate does not match the hostname the client was trying to access.  <b>Note</b> 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 <a href="http://www.openssl.org/docs/apps/verify.html">http://www.openssl.org/docs/apps/verify.html</a> .

**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.



The Web Security appliance only performs the OCSP query for certificates that it determines to be valid in all other respects and that include the OCSP URL.

### Related Topics

- [Enabling Real-Time Revocation Status Checking, page 7-12](#)
- [Configuring Invalid Certificate Handling, page 7-10](#)

## Enabling Real-Time Revocation Status Checking

### Before You Begin

- Ensure the HTTPS Proxy is enabled. See [Enabling the HTTPS Proxy, page 7-3](#)

**Step 1** Security Services > HTTPS Proxy.

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

**Step 3** Select **Enable Online Certificate Status Protocol (OCSP)**.

**Step 4** Configure the **OCSP Result Handling** properties,

Cisco recommends configuring the OCSP Result Handling options to the same actions as Invalid Certificate Handling options. For example, if you set Expired Certificate to Monitor, configure Revoked Certificate to monitor.

**Step 5** (Optional) Expand the Advanced configuration section and configure the settings described below.

Field Name	Description
OCSP Valid Response Cache Timeout	Time to wait before rechecking a valid OCSP response in seconds (s), minutes (m), hours (h), or days (d). Default unit is seconds. Valid range is from 1 second to 7 days.
OCSP Invalid Response Cache Timeout	Time to wait before rechecking an invalid OCSP response in seconds (s), minutes (m), hours (h), or days (d). Default unit is seconds. Valid range is from 1 second to 7 days.
OCSP Network Error Cache Timeout	Time to wait before attempting to contact the OCSP responder again after failing to get a response in seconds (s), minutes (m), hours (h), or days (d). Valid range from 1 second to 24 hours.
Allowed Clock Skew	Maximum allowed difference in time settings between the Web Security appliance and the OCSP responder in seconds (s) or minutes (m). Valid range from 1 second to 60 minutes.
Maximum Time to Wait for OCSP Response	Maximum time to wait for a response from the OCSP responder. Valid range is from 1 second to 10 minutes. Specify a shorter duration to reduce delays in end user access to HTTPS requests in the event that the OCSP responder is unavailable.
Use upstream proxy for OCSP checking	Group Name of the upstream proxies.
Servers exempt from upstream proxy	IP addresses or hostnames of the servers to exempt. May be left blank.

**Step 6** Submit and Commit Changes.

## Trusted Root Certificates

The Web Security appliance ships with and maintains a list of trusted root certificates. Web sites with trusted certificates do not require decryption.

You can manage the trusted certificate list, adding certificates to it and functionally removing certificates from it. While the Web Security appliance does not delete certificates from the master list, it allows you to override trust in a certificate, which functionally removes the certificate from the trusted list.

## Adding Certificates to the Trusted List

### Before You Begin

- Verify that the HTTPS Proxy is enabled. See [Enabling the HTTPS Proxy, page 7-3](#)

---

**Step 1** **Security Services > HTTPS Proxy.**

**Step 2** Click **Manage Trusted Root Certificates**.

**Step 3** Click **Import**.

**Step 4** Click **Browse** and navigate to the certificate file.

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

Look for the certificate you uploaded in the **Custom Trusted Root Certificates** list.

---

## Removing Certificates from the Trusted List

---

**Step 1** Select **Security Services > HTTPS Proxy**.

**Step 2** Click **Manage Trusted Root Certificates**.

**Step 3** Select the **Override Trust** checkbox corresponding to the certificate you wish to remove from the list.

**Step 4** **Submit and Commit Changes.**

---

## Routing HTTPS Traffic

The ability of AsyncOS to route HTTPS transactions based on information stored in client headers is limited and is different for transparent and explicit HTTPS.

Option	Description
Transparent HTTPS	In the case of transparent HTTPS, AsyncOS does not have access to information in the client headers. Therefore, AsyncOS cannot enforce routing policies that rely on information in client headers.
Explicit HTTPS	In the case of explicit HTTPS, AsyncOS has access to the following information in client headers: <ul style="list-style-type: none"><li>URL</li><li>Destination port number</li></ul> Therefore, for explicit HTTPS transactions, it is possible to match a routing policy based on URL or port number.

# Troubleshooting Decryption/HTTPS/Certificates

- Accessing HTTPS Sites Using Routing Policies with URL Category Criteria, page A-6
- HTTPS with IP-based Surrogates and Transparent Requests, page A-6
- Bypassing Decryption for Particular Websites, page A-7
- Alert: Problem with Security Certificate, page A-8



# Configuring Security Services

- [Overview of Web Reputation Filters, page 8-1](#)
- [Overview of Anti-Malware Scanning, page 8-3](#)
- [Understanding Adaptive Scanning, page 8-5](#)
- [Maintaining the Database Tables, page 8-6](#)
- [Logging of Web Reputation Filtering Activity and DVS Scanning, page 8-6](#)
- [Caching, page 8-7](#)
- [Malware Category Descriptions, page 8-7](#)

## Overview of Web Reputation Filters

Web Reputation Filters assigns a web-based reputation score (WBRS) to a URL to determine the likelihood that it contains URL-based malware. The Web Security appliance uses web reputation scores to identify and stop malware attacks before they occur. You can use Web Reputation Filters with Access, Decryption, and Cisco IronPort Data Security Policies.

## Web Reputation Scores

Web Reputation Filters use data to assess the reliability of Internet domains and score the reputation of URLs. The web reputation calculation associates a URL with network parameters to determine the probability that malware exists. The aggregate probability that malware exists is then mapped to a Web Reputation Score between -10 and +10, with +10 being the least likely to contain malware.

Example parameters include the following:

- URL categorization data
- Presence of downloadable code
- Presence of long, obfuscated End-User License Agreements (EULAs)
- Global volume and changes in volume
- Network owner information
- History of a URL
- Age of a URL
- Presence on any block lists

- Presence on any allow lists
- URL typos of popular domains
- Domain registrar information
- IP address information



**Note** Cisco does not collect identifiable information such as user names, 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
Cisco IronPort Data Security Policies	You can choose to block or monitor

## Web Reputation in Access Policies

When you configure web reputation settings in Access Policies, you can choose to configure the settings manually, or let AsyncOS for Web choose the best options using Adaptive Scanning. When Adaptive Scanning is enabled, you can enable or disable web reputation filtering in each Access Policy, but you cannot edit the Web Reputation Scores.

Score	Action	Description	Example
-10 to -6.0	Block	Bad site. The request is blocked, and no further malware scanning occurs.	<ul style="list-style-type: none"> <li>• URL downloads information without user permission.</li> <li>• Sudden spike in URL volume.</li> <li>• URL is a typo of a popular domain.</li> </ul>
-5.9 to 5.9	Scan	Undetermined site. Request is passed to the DVS engine for further malware scanning. The DVS engine scans the request and server response content.	<ul style="list-style-type: none"> <li>• Recently created URL that has a dynamic IP address and contains downloadable content.</li> <li>• Network owner IP address that has a positive Web Reputation Score.</li> </ul>
6.0 to 10.0	Allow	Good site. Request is allowed. No malware scanning required.	<ul style="list-style-type: none"> <li>• URL contains no downloadable content.</li> <li>• Reputable, high-volume domain with long history.</li> <li>• Domain present on several allow lists.</li> <li>• No links to URLs with poor reputations.</li> </ul>

By default, URLs in an HTTP request that are assigned a Web Reputation Score of +7 are allowed and require no further scanning. However, a weaker score for an HTTP request, such as +3, is automatically forwarded to the Cisco IronPort DVS engine where it is scanned for malware. Any URL in an HTTP request that has a poor reputation is blocked.

#### Related Topics

- [Understanding Adaptive Scanning, page 8-5](#)

## Web Reputation in Cisco IronPort Data Security Policies

Score	Action	Description
-10 to -6.0	Block	Bad site. The transaction is blocked, and no further scanning occurs.
-5.9 to 0.0	Monitor	The transaction will not be blocked based on Web Reputation, and will proceed to content checks (file type and size).
<b>Note</b>		Sites with no score are monitored.

## Overview of Anti-Malware Scanning

The Web Security appliance anti-malware feature uses the Cisco IronPort DVS™ engine in combination with anti-malware scanning engines to stop web-based malware threats. The DVS engine works with the Webroot™, McAfee, and Sophos anti-malware scanning engines.

The scanning engines inspect transactions to determine a malware scanning verdict to pass to the DVS engine. The DVS engine determines whether to monitor or block the request based on the malware scanning verdicts. To use the anti-malware component of the appliance, you must enable anti-malware scanning and configure global settings, and then apply specific settings to different policies.

## 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.

## Maintaining the Database Tables

The web reputation, Webroot, Sophos, and McAfee databases periodically receive updates from the Cisco IronPort 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 explains 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 user's consent.

**■ Malware Category Descriptions**

<b>Malware Type</b>	<b>Description</b>
Known Malicious and High-Risk Files	These are files that were identified as threats by the Advanced Malware Protection file reputation service.
Other Malware	This category is used to catch all other malware and suspicious behavior that does not exactly fit in one of the other defined categories.
Phishing URL	A phishing URL is displayed in the browser address bar. In some cases, it involves the use of domain names and resembles those of legitimate domains.
PUA	Potentially Unwanted Application. A PUA is an application that is not malicious, but may be considered to be undesirable.
System Monitor	A system monitor encompasses any software that performs one of the following: <ul style="list-style-type: none"> <li>• Overtly or covertly records system processes and/or user action.</li> <li>• Makes those records available for retrieval and review at a later time.</li> </ul>
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.



## Notify End-Users of Proxy Actions

- [End-User Notifications Overview, page 9-1](#)
- [Configuring General Settings for Notification Pages, page 9-2](#)
- [End-User Acknowledgment Page, page 9-2](#)
- [End-User Notification Pages, page 9-5](#)
- [Configuring the End-User URL Filtering Warning Page, page 9-9](#)
- [Configuring FTP Notification Messages, page 9-9](#)
- [Custom Messages on Notification Pages, page 9-10](#)
- [Editing Notification Page HTML Files Directly, page 9-12](#)
- [Notification Page Types, page 9-15](#)

## 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.	<a href="#">End-User Acknowledgment Page, page 9-2</a>
End-user notification pages	Page shown to end users when access to a particular page is blocked, specific to the reason for blocking it.	<a href="#">End-User Notification Pages, page 9-5</a>
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.	<a href="#">Configuring the End-User URL Filtering Warning Page, page 9-9</a>

## Configuring General Settings for Notification Pages

Option	Description	Further information
FTP notification messages	Gives end users the reason a native FTP transaction was blocked.	<a href="#">Configuring FTP Notification Messages, page 9-9.</a>
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.  See also <a href="#">Time Ranges and Quotas, page 10-16.</a>

# Configuring General Settings for Notification Pages

Specify display languages and logo for notification pages. Restrictions are described in this 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.

## Related Topics

- [Caveats for URLs and Logos in Notification Pages, page 9-11](#)

# 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

The end-user acknowledgment page works because it displays an HTML page to the end user that forces them to click an acceptable use policy agreement. After users click the link, the Web Proxy redirects clients to the originally requested website. It keeps track of when users accepted the end-user acknowledgment page using a surrogate (either by IP address or web browser session cookie) if no username is available for the user.

- **HTTPS.** The Web Proxy tracks whether the user has acknowledged the end-user acknowledgment page with a cookie, but it cannot obtain the cookie unless it decrypts the transaction. You can choose to either bypass (pass through) or drop HTTPS requests when the end-user acknowledgment page is enabled and tracks users using session cookies. Do this using the `advancedproxyconfig > EUN CLI` command, and choose bypass for the “Action to be taken for HTTPS requests with Session based EUA (“bypass” or “drop”).” command.
- **FTP over HTTP.** Web browsers never send cookies for FTP over HTTP transactions, so the Web Proxy cannot obtain the cookie. To work around this, you can exempt FTP over HTTP transactions from requiring the end-user acknowledgment page. Do this by creating a custom URL category using “`ftp://`” as the regular expression (without the quotes) and defining an Identity policy that exempts users from the end-user acknowledgment page for this custom URL category.

## 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

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`.

### Before You Begin

- To configure the display language and customize the displayed logo, see [Configuring General Settings for Notification Pages, page 9-2](#).

**■ End-User Acknowledgment Page**

- If you will customize the message shown to end users, see [Custom Messages on Notification Pages, page 9-10](#). If you require more customization than the Custom Message box allows, see [Editing Notification Page HTML Files Directly, page 9-12](#).

**Step 1** Security Services > End-User Notification.

**Step 2** Click Edit Settings.

**Step 3** Enable the “Require end-user to click through acknowledgment page” field.

**Step 4** Enter options:

Setting	Description
<b>Time Between Acknowledgements</b>	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).  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.
<b>Inactivity Timeout</b>	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
<b>Surrogate Type</b>	<p>Determines which method the Web Proxy uses to track the user:</p> <ul style="list-style-type: none"> <li>• <b>IP Address.</b> 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.</li> </ul> <p><b>Note</b> When IP address is configured and the user is authenticated, the Web Proxy tracks users by username instead of IP address.</p> <ul style="list-style-type: none"> <li>• <b>Session Cookie.</b> 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.</li> </ul> <p>If the user using a non-browser HTTP client application, they must be able to click the link on the end-user acknowledgment page to access the web. If the user opens a second web browser application, the user must go through the end-user acknowledgment process again in order for the Web Proxy to send a session cookie to the second web browser.</p> <p><b>Note</b> Using a session cookie to track users when the client accesses HTTPS sites or FTP servers using FTP over HTTP is not supported.</p>
<b>Custom message</b>	<p>Customize the text that appears on every end-user acknowledgment page. You can include some simple HTML tags to format the text.</p> <p><b>Note</b> You can only include a custom message when you configure the end-user acknowledgment page in the web interface, versus the CLI.</p> <p>See also <a href="#">Custom Messages on Notification Pages, page 9-10</a>.</p>

**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.	<a href="#">Configuring On-Box End-User Notification Pages, page 9-6</a>
Redirect the user to HTTP end-user notification pages at a specific URL.	<a href="#">Off-Box End-User Notification Pages, page 9-7</a>

## Configuring On-Box End-User Notification Pages

On-box pages are predefined, customizable notification pages residing on the appliance.

### Before You Begin

- To configure the display language and customize the displayed logo, see [Configuring General Settings for Notification Pages, page 9-2](#).
- If you will customize the message displayed using on-box notifications, review the topics under [Custom Messages on Notification Pages, page 9-10](#). If you require more customization than the Custom Message box allows, see [Editing Notification Page HTML Files Directly, page 9-12](#).

---

**Step 1** **Security Services > End-User Notification.**

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

**Step 3** From the Notification Type field, choose **Use On Box End User Notification**.

**Step 4** Configure the on-box end-user notification page settings.

Setting	Description
Custom Message	Include any additional text required on each notification page. When you enter a custom message, AsyncOS places the message before the last sentence on the notification page which includes the contact information.
Contact Information	Customize the contact information listed on each notification page. AsyncOS displays the contact information sentence as the last sentence on a page, before providing notification codes that users can provide to the network administrator.
End-User Misclassification Reporting	When enabled, users can report misclassified URLs to Cisco. An additional button appears on the on-box end-user notification pages for sites blocked due to suspected malware or URL filters. This button allows the user to report when they believe the page has been misclassified. It does not appear for pages blocked due to other policy settings.

**Step 5** (Optional) Click **Preview Notification Page Customization** link to view the current end-user notification page in a separate browser window.



**Note** If the 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

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, page 9-7](#).

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
```

**End-User Notification Pages**

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. <b>Note:</b> AsyncOS for Web sends the entire URL category name for both predefined and user defined URL categories. It performs URL encoding on the category name, so spaces are written as "%20".
WBRS	WBRS score that the Web Reputation Filters assigned to the URL in the request.
DVS_Verdict	Malware category that the DVS engine assigns to the transaction.
DVS_ThreatName	The name of the malware found by the DVS engine.
Reauth_URL	A URL that users can click to authenticate again if the user is blocked from a website due to a restrictive URL filtering policy. Use this parameter when the "Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction" global authentication setting is enabled and the user is blocked from a website due to a blocked URL category. To use this parameter, make sure the CGI script performs the following steps: 1. Get the value of <code>Reauth_Url</code> parameter. 2. URL-decode the value. 3. Base64 decode the value and get the actual re-authentication URL. 4. Include the decoded URL on the end-user notification page in some way, either as a link or button, along with instructions for users informing them they can click the link and enter new authentication credentials that allow greater access.



**Note** AsyncOS always includes all parameters in each redirected URL. If no value exists for a particular parameter, AsyncOS passes a hyphen (-).

## Redirecting End-User Notification Pages to a Custom URL (Off-Box)

- 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

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.

### Before You Begin

If you will customize the message displayed using on-box notifications, review the topics under [Custom Messages on Notification Pages, page 9-10](#). If you require more customization than the Custom Message box allows, see [Editing Notification Page HTML Files Directly, page 9-12](#).

- 
- 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

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.

**Before You Begin**

If you will customize the message displayed using on-box notifications, review the topics under [Custom Messages on Notification Pages, page 9-10](#). If you require more customization than the Custom Message box allows, see [Editing Notification Page HTML Files Directly, page 9-12](#).

- 
- 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, page 9-10](#)
- [Caveats for URLs and Logos in Notification Pages, page 9-11](#)

## 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>
- <span></span>
- <b></b>
- <big></big>
- <br>
- <code></code>
- <em></em>
- <i></i>
- <small></small>
- <strong></strong>

For example, you can make some text italic:

Please acknowledge the following statements <i>before</i> accessing the Internet.

With the <span> 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, page 9-12](#).

## 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

- 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, page 9-10](#).
- The customized notification page file names must exactly match the file names shipped with the Web Security appliance.  
If the `configuration\ewn` 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, page 9-12](#).
- See [Variables for Customizing Notification HTML Files](#) and [Using Variables in Notification HTML Files, page 9-13](#).

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Use an FTP client to connect to the Web Security appliance.  |
| <b>Step 2</b> | Navigate to the <code>configuration\ewn</code> directory.  |
| <b>Step 3</b> | Download the language directory files for the notification pages you want to edit.                                     |
| <b>Step 4</b> | On your local machine, use a text or HTML editor to edit the HTML files.   |
| <b>Step 5</b> | Use the FTP client to upload the customized HTML files to the same directory from which you downloaded them in step 3. |
| <b>Step 6</b> | Open an SSH client and connect to the Web Security appliance.  |
| <b>Step 7</b> | Run the <code>advancedproxyconfig &gt; EUN</code> CLI command.   |
| <b>Step 8</b> | Type <code>2</code> 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:  else Use this with the %?V conditional variable.
%#V	Represents the following condition:  endif 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](#) 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, page 9-13](#).

## ■ Editing Notification Page HTML Files Directly

<b>Variable</b>	<b>Description</b>	<b>Always Evaluates to TRUE if Used as Conditional Variable</b>
%a	Authentication realm for FTP	No
%A	ARP address	Yes
%b	User-agent name	No
%B	Blocking reason, such as BLOCK-SRC or BLOCK-TYPE	No
%c	Error page contact person	Yes
%C	Entire Set-Cookie: header line, or empty string	No
%d	Client IP address	Yes
%D	User name	No
%e	Error page email address	Yes
%E	The error page logo URL	No
%f	User feedback section	No
%F	The URL for user feedback	No
%g	The web category name, if available	Yes
%G	Maximum file size allowed in MB	No
%h	The hostname of the proxy	Yes
%H	The server name of the URL	Yes
%i	Transaction ID as a hexadecimal number	Yes
%I	Management IP Address	Yes
%j	URL category warning page custom text	No
%k	Redirection link for the end-user acknowledgment page and end-user URL filtering warning page	No
%K	Response file type	No
%l	WWW-Authenticate: header line	No
%L	Proxy-Authenticate: header line	No
%M	The Method of the request, such as “GET” or “POST”	Yes
%n	Malware category name, if available	No
%N	Malware threat name, if available	No
%o	Web reputation threat type, if available	No
%O	Web reputation threat reason, if available	No
%p	String for the Proxy-Connection HTTP header	Yes
%P	Protocol	Yes
%q	Identity policy group name	Yes
%Q	Policy group name for non-Identity policies	Yes
%r	Redirect URL	No

Variable	Description	Always Evaluates to TRUE if Used as Conditional Variable
%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](#).

The table describes the different notification pages users might encounter.

File Name and Notification Title	Notification Description	Notification Text
ERR_ACCEPTED Feedback Accepted, Thank You	Notification page that is displayed after the users uses the “Report Misclassification” option.	The misclassification report has been sent. Thank you for your feedback.
ERR_ADAPTIVE_SECURITY Policy: General	Block page that is displayed when the user is blocked due to the Adaptive Scanning feature.	Based on your organization’s security policies, this web site <URL> has been blocked because its content has been determined to be a security risk.

## ■ Notification Page Types

File Name and Notification Title	Notification Description	Notification Text
ERR_ADULT_CONTENT Policy Acknowledgment	The warning page that is displayed when the end-user accesses a page that is classified as adult content. Users can click an acknowledgment link to continue to the originally requested site.	<p>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.</p> <p>Click here to accept this statement and access the Internet.</p>
ERR_AVC Policy: Application Controls	Block page that is displayed when the user is blocked due to the Application Visibility and Control engine.	Based on your organization's access policies, access to application %1 of type %2 has been blocked.
ERR_BAD_REQUEST Bad Request	Error page that results from an invalid transaction request.	<p>The system cannot process this request. A non-standard browser may have generated an invalid HTTP request.</p> <p>If you are using a standard browser, please retry the request.</p>
ERR_BLOCK_DEST Policy: Destination	Block page that is displayed when the user tries to access a blocked website address.	Based on your organization's Access Policies, access to this web site <URL> has been blocked.
ERR_BROWSER Security: Browser	Block page that is displayed when the transaction request comes from an application that has been identified to be compromised by malware or spyware.	<p>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 "&lt;malware name&gt;".</p> <p>Please contact &lt;contact name&gt; &lt;email address&gt; and provide the codes shown below.</p> <p>If you are using a non-standard browser and believe it has been misclassified, use the button below to report this misclassification.</p>
ERR_BROWSER_CUSTO M 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 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.

File Name and Notification Title	Notification Description	Notification Text
ERR_CONTINUE_UNACKNOWLEDGED Policy Acknowledgment	Warning page that is displayed when the user requests a site that is in a custom URL category that is assigned the Warn action. Users can click an acknowledgment link to continue to the originally requested site.	<p>You are trying to visit a web page that falls under the URL Category &lt;URL category&gt;. 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.</p> <p>Click here to accept this statement and access the Internet.</p>
ERR_DNS_FAIL DNS Failure	Error page that is displayed when the requested URL contains an invalid domain name.	<p>The hostname resolution (DNS lookup) for this hostname &lt;hostname&gt; has failed. The Internet address may be misspelled or obsolete, the host &lt;hostname&gt; may be temporarily unavailable, or the DNS server may be unresponsive.</p> <p>Please check the spelling of the Internet address entered. If it is correct, try this request later.</p>
ERR_EXPECTATION_FAILED Expectation Failed	Error page that is displayed when the transaction request triggers the HTTP 417 “Expectation Failed” response.	<p>The system cannot process the request for this site &lt;URL&gt;. A non-standard browser may have generated an invalid HTTP request.</p> <p>If using a standard browser, please retry the request.</p>
ERR_FILE_SIZE Policy: File Size	Block page that is displayed when the requested file is larger than the allowed maximum file size.	Based on your organization's Access Policies, access to this web site or download <URL> has been blocked because the download size exceeds the allowed limit.
ERR_FILE_TYPE Policy: File Type	Block page that is displayed when the requested file is a blocked file type.	Based on your organization's Access Policies, access to this web site or download <URL> has been blocked because the file type “<file type>” is not allowed.
ERR_FILTER_FAILURE Filter Failure	Error page that is displayed when the URL filtering engine is temporarily unable to deliver a URL filtering response and the “Default Action for Unreachable Service” option is set to Block.	<p>The request for page &lt;URL&gt; has been denied because an internal server is currently unreachable or overloaded.</p> <p>Please retry the request later.</p>
ERR_FOUND Found	Internal redirection page for some errors.	The page <URL> is being redirected to <redirected URL>.
ERR_FTP_ABORTED FTP Aborted	Error page that is displayed when the FTP over HTTP transaction request triggers the HTTP 416 “Requested Range Not Satisfiable” response.	<p>The request for the file &lt;URL&gt; did not succeed. The FTP server &lt;hostname&gt; unexpectedly terminated the connection.</p> <p>Please retry the request later.</p>

## ■ Notification Page Types

File Name and Notification Title	Notification Description	Notification Text
ERR_FTP_AUTH_REQIRED  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.  In some cases, the FTP server may limit the number of anonymous connections. If you usually connect to this server as an anonymous user, please try again later.
ERR_FTP_CONNECTION_FAILED  FTP Connection Failed	Error page that is displayed when the FTP over HTTP transaction request triggers the FTP 425 “Can’t open data connection” response.	The system cannot communicate with the FTP server <hostname>. The FTP server may be temporarily or permanently down, or may be unreachable because of network problems.  Please check the spelling of the address entered. If it is correct, try this request later.
ERR_FTP_FORBIDDEN  FTP Forbidden	Error page that is displayed when the FTP over HTTP transaction request is for an object the user is not allowed to access.	Access was denied by the FTP server <hostname>. Your user ID does not have permission to access this document.
ERR_FTP_NOT_FOUND  FTP Not Found	Error page that is displayed when the FTP over HTTP transaction request is for an object that does not exist on the server.	The file <URL> could not be found. The address is either incorrect or obsolete.
ERR_FTP_SERVER_ERR  FTP Server Error	Error page that is displayed for FTP over HTTP transactions that try to access a server that does support FTP. The server usually returns the HTTP 501 “Not Implemented” response.	The system cannot communicate with the FTP server <hostname>. The FTP server may be temporarily or permanently down, or may not provide this service.  Please confirm that this is a valid address. If it is correct, try this request later.
ERR_FTP_SERVICE_UNAVAIL  FTP Service Unavailable	Error page that is displayed for FTP over HTTP transactions that try to access an FTP server that is unavailable.	The system cannot communicate with the FTP server <hostname>. The FTP server may be busy, may be permanently down, or may not provide this service.  Please confirm that this is a valid address. If it is correct, try this request later.
ERR_GATEWAY_TIMEOUT  Gateway Timeout	Error page that is displayed when the requested server has not responded in a timely manner.	The system cannot communicate with the external server <hostname>. The Internet server may be busy, may be permanently down, or may be unreachable because of network problems.  Please check the spelling of the Internet address entered. If it is correct, try this request later.
ERR_IDS_ACCESS_FORBIDDEN  IDS Access Forbidden	Block page that is displayed when the user tries to upload a file that is blocked due to a configured Cisco Data Security Policy.	Based on your organization’s data transfer policies, your upload request has been blocked. File details: <file details>

File Name and Notification Title	Notification Description	Notification Text
ERR_INTERNAL_ERRO R  Internal Error	Error page that is displayed when there is an internal error.	Internal system error when processing the request for the page <URL>. Please retry this request. If this condition persists, please contact <contact name> <email address> and provide the code shown below.
ERR_MALWARE_SPECIFIC FIC  Security: Malware Detected	Block page that is displayed when malware is detected when downloading a file.	Based on your organization's Access Policies, this web site <URL> has been blocked because it has been determined to be a security threat to your computer or the organization's network. Malware <malware name> in the category <malware category> has been found on this site.
ERR_MALWARE_SPECIFIC_OUTGOING  Security: Malware Detected	Block page that is displayed when malware is detected when uploading a file.	Based on your organization's policy, the upload of the file to URL (<URL>) has been blocked because the file was detected to contain malware that will be harmful to the receiving end's network security. Malware Name: <malware name> Malware Category: <malware category>
ERR_NATIVE_FTP_DENIED	Block message displayed in native FTP clients when the native FTP transaction is blocked.	530 Login denied
ERR_NO_MORE_FORWARDS  No More Forwards	Error page that is displayed when the appliance has detected a forward loop between the Web Proxy and another proxy server on the network. The Web Proxy breaks the loop and displays this message to the client.	The request for the page <URL> failed. The server address <hostname> may be invalid, or you may need to specify a port number to access this server.
ERR_POLICY Policy: General	Block page that is displayed when the request is blocked by any policy setting.	Based on your organization's Access Policies, access to this web site <URL> has been blocked.
ERR_PROTOCOL Policy: Protocol	Block page that is displayed when the request is blocked based on the protocol used.	Based on your organization's Access Policies, this request has been blocked because the data transfer protocol "<protocol type>" is not allowed.
ERR_PROXY_AUTH_REQUIRED  Proxy Authorization Required	Notification page that is displayed when users must enter their authentication credentials to continue. This is used for explicit transaction requests.	Authentication is required to access the Internet using this system. A valid user ID and passphrase must be entered when prompted.

**■ Notification Page Types**

File Name and Notification Title	Notification Description	Notification Text
ERR_PROXY_PREVENT _MULTIPLE_LOGIN  Already Logged In From Another Machine	Block page that is displayed when someone tries to access the web using the same username that is already authenticated with the Web Proxy on a different machine. This is used when the User Session Restrictions global authentication option is enabled.	Based on your organization's policies, the request to access the Internet was denied because this user ID has an active session from another IP address.  If you want to login as a different user, click on the button below and enter a different user name and passphrase.
ERR_PROXY_REDIRECT  Redirect	Redirection page.	This request is being redirected. If this page does not automatically redirect, click here to proceed.
ERR_PROXY_UNACKNO WLEDGED  Policy Acknowledgment	End-user acknowledgment page.  For more information, see <a href="#">End-User Notification Pages, page 9-5</a> .	Please acknowledge the following statements before accessing the Internet.  Your web transactions will be automatically monitored and processed to detect dangerous content and to enforce organization's policies. By clicking the link below, you acknowledge this monitoring and accept that data about the sites you visit may be recorded. You will be periodically asked to acknowledge the presence of the monitoring system. You are responsible for following organization's polices on Internet access.  Click here to accept this statement and access the Internet.
ERR_PROXY_UNLICEN SED  Proxy Not Licensed	Block page that is displayed when there is no valid license key for the Web Security appliance Web Proxy.	Internet access is not available without proper licensing of the security device.  Please contact <contact name> <email address> and provide the code shown below.  <b>Note</b> To access the management interface of the security device, enter the configured IP address with port.
ERR_RANGE_NOT_SATI SFIABLE  Range Not Satisfiable	Error page that is displayed when the requested range of bytes cannot be satisfied by the web server.	The system cannot process this request. A non-standard browser may have generated an invalid HTTP request.  If you are using a standard browser, please retry the request.
ERR_REDIRECT_PERM ANENT  Redirect Permanent	Internal redirection page.	The page <URL> is being redirected to <redirected URL>.
ERR_REDIRECT_REPEA T_REQUEST  Redirect	Internal redirection page.	Please repeat your request.

File Name and Notification Title	Notification Description	Notification Text
ERR_SAAS_AUTHENTICATION Policy: Access Denied	Notification page that is displayed when users must enter their authentication credentials to continue. This is used for accessing applications.	Based on your organization's policy, the request to access <URL> was redirected to a page where you must enter the login credentials. You will be allowed to access the application if authentication succeeds and you have the proper privileges.
ERR_SAAS_AUTHORIZATION Policy: Access Denied	Block page that is displayed when users try to access a application that they have no privilege to access.	Based on your organization's policy, the access to the application <URL> is blocked because you are not an authorized user. If you want to login as a different user, enter a different username and passphrase for a user that is authorized to access this application.
ERR_SAML_PROCESSING Policy: Access Denied	Error page that is displayed when an internal process fails trying to process the single sign-on URL for accessing a application.	The request to access <user name> did not go through because errors were found during the process of the single sign on request.
ERR_SERVER_NAME_EXPANSION Server Name Expansion	Internal redirection page that automatically expands the URL and redirects users to the updated URL.	The server name <hostname> appears to be an abbreviation, and is being redirected to <redirected URL>.
ERR_URI_TOO_LONG URI Too Long	Block page that is displayed when the URL length is too long.	The requested URL was too long and could not be processed. This may represent an attack on your network.  Please contact <contact name> <email address> and provide the code shown below.
ERR_WBRS Security: Malware Risk	Block page that is displayed when the Web Reputation Filters block the site due to a low web reputation score.	Based on your organization's access policies, this web site <URL> has been blocked because it has been determined by Web Reputation Filters to be a security threat to your computer or the organization's network. This web site has been associated with malware/spyware.  Threat Type: %o  Threat Reason: %O
ERR_WEBCAT Policy: URL Filtering	Block page that is displayed when users try to access a website in a blocked URL category.	Based on your organization's Access Policies, access to this web site <URL> has been blocked because the web category "<category type>" is not allowed.
ERR_WWW_AUTH_REQUIRED 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.

**■ Notification Page Types**



## Web Security Appliance Reports

---

- [Overview Page, page 10-1](#)
- [System Capacity Page, page 10-1](#)
- [System Status Page, page 10-2](#)

### Overview Page

The System Status page, displayed when you log in or click the Home button, provides a “snapshot” of the appliance status, cloud communications status, and configuration information.

### 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 a minute by minute basis over a 60 minute period.
- **Day Report.** The Day report queries the hour table and displays the exact number of items, such as bytes and connection, that have been recorded by the appliance on an hourly basis over a 24 hour period. This information is gathered from the hour table.

The Week Report and 30 Days Report work similarly to the Hour and Day Reports.

# System Status Page

Use the **Reporting > System Status** page to monitor the System Status. This page displays the current status and configuration of the Web Security appliance.

This Section...	Displays
Web Security Appliance Status	<ul style="list-style-type: none"> <li>System uptime</li> <li>System resource utilization — CPU usage, RAM usage, and percentage of disk space used for reporting and logging.</li> </ul> <p>The CPU utilization value shown on this page and the CPU value shown on the system Overview page (<a href="#">Overview Page, page 10-1</a>) may differ slightly because they are read separately, at differing moments.</p> <p>RAM usage for a system that is working efficiently may be above 90%, because RAM that is not otherwise in use by the system is used by the web object cache. If your system is not experiencing serious performance issues and this value is not stuck at 100%, the system is operating normally.</p> <p><b>Note</b> Proxy Buffer Memory is one component that uses this RAM.</p>
Proxy Traffic Characteristics	<ul style="list-style-type: none"> <li>Transactions per second</li> <li>Bandwidth</li> <li>Response time</li> <li>Cache hit rate</li> <li>Connections</li> </ul>
High Availability	
External Services	<ul style="list-style-type: none"> <li>Identity Services Engine</li> </ul>
Current Configuration	<p>Web Proxy settings:</p> <ul style="list-style-type: none"> <li>Web Proxy Status — enabled or disabled.</li> <li>Deployment Topology.</li> <li>Web Proxy Mode — forward or transparent.</li> </ul> <p>L4 Traffic Monitor settings:</p> <ul style="list-style-type: none"> <li>L4 Traffic Monitor Status — enabled or disabled.</li> <li>L4 Traffic Monitor Wiring.</li> <li>L4 Traffic Monitor Action — monitor or block.</li> </ul> <p>Web Security Appliance Version Information</p> <p>Hardware information</p>

## Related Topics

- [System Capacity Page, page 10-1](#)



# Monitor System Activity Through Logs

- [Overview of Logging, page 11-1](#)
- [Common Tasks for Logging, page 11-2](#)
- [Best Practices for Logging, page 11-2](#)
- [Troubleshooting Web Proxy Issues Using Logs, page 11-2](#)
- [Log File Types, page 11-3](#)
- [Adding and Editing Log Subscriptions, page 11-7](#)
- [Pushing Log Files to Another Server, page 11-11](#)
- [Archiving Log Files, page 11-11](#)
- [Log File Names and Appliance Directory Structure, page 11-12](#)
- [Viewing Log Files, page 11-13](#)
- [Web Proxy Information in Access Log Files, page 11-13](#)
- [Interpreting Access Log Scanning Verdict Entries, page 11-20](#)
- [W3C Compliant Access Log Files, page 11-24](#)
- [Customizing Access Logs, page 11-26](#)
- [Traffic Monitor Log Files, page 11-29](#)
- [Log File Fields and Tags, page 11-30](#)
- [Troubleshooting Logging, page 11-41](#)

## 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.

**Common Tasks for Logging**

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, page 11-2](#)
- [Log File Types, page 11-3](#)

## Common Tasks for Logging

Task	Links to Related Topics and Procedures
Troubleshoot web proxy issues using logs	<a href="#">Troubleshooting Web Proxy Issues Using Logs, page 11-2</a>
Add and edit log subscriptions	<a href="#">Adding and Editing Log Subscriptions, page 11-7</a>
View log files	<a href="#">Viewing Log Files, page 11-13</a>
Interpret log files	<a href="#">Interpreting Access Log Scanning Verdict Entries, page 11-20</a>
Customize log files	<a href="#">Customizing Access Logs, page 11-26</a>
Push log files to another server	<a href="#">Pushing Log Files to Another Server, page 11-11</a>
Archiving log files	<a href="#">Archiving Log Files, page 11-11</a>

## 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.

---

**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
Hybrid Service Logs	Webroot Integration Framework Logs
License Module Logs	

- Step 3** Recreate the issue and read the new Web Proxy module log for relevant entries.
- Step 4** Repeat as required with other Web Proxy module logs.
- Step 5** Remove subscriptions that are no longer required.
- 

#### Related Topics

- [Log File Types, page 11-3](#)
- [Adding and Editing Log Subscriptions, page 11-7](#)

## 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.) See also <a href="#">Log Files, page 14-17</a> .	Yes	Yes
Audit Logs	Records AAA (Authentication, Authorization, and Accounting) events. Records all user interaction with the application and command-line interfaces, and captures committed changes.	Yes	Yes
Access Logs	Records Web Proxy client history.	Yes	Yes

**Log File Types**

<b>Log File Type</b>	<b>Description</b>	<b>Supports Syslog Push?</b>	<b>Enabled by Default?</b>
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
Data Security Logs	Records client history for upload requests that are evaluated by the Cisco Data Security Filters.	Yes	Yes
Data Security Module Logs	Records messages related to the Cisco Data Security Filters.	No	No
DCA Engine Framework Logs (Dynamic Content Analysis)	Records messages related to communication between the Web Proxy and the Cisco Web Usage Controls Dynamic Content Analysis engine.	No	No
DCA Engine Logs (Dynamic Content Analysis)	Records messages related to the Cisco Web Usage Controls Dynamic Content Analysis engine.	Yes	Yes
Default Proxy Logs	Records errors related to the Web Proxy.  This is the most basic of all Web Proxy related logs. To troubleshoot more specific aspects related to the Web Proxy, create a log subscription for the applicable Web Proxy module.	Yes	Yes
Disk Manager Logs	Records Web Proxy messages related to writing to the cache on disk.	No	No
External Authentication Logs	Records messages related to using the external authentication feature, such as communication success or failure with the external authentication server.  Even with external authentication is disabled, this log contains messages about local users successfully or failing logging in.	No	Yes
Feedback Logs	Records the web users reporting misclassified pages.	Yes	Yes
FTP Proxy Logs	Records error and warning messages related to the FTP Proxy.	No	No
FTP Server Logs	Records all files uploaded to and downloaded from the Web Security appliance using FTP.	Yes	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
GUI Logs (Graphical User Interface)	Records history of page refreshes in the web interface. GUI logs also include information about SMTP transactions, for example information about scheduled reports emailed from the appliance.	Yes	Yes
Haystack Logs	Haystack logs record web transaction tracking data processing.	Yes	Yes
Hybrid Service Logs	Records all communications between appliance and ScanCenter portal, as well as with hybrid registration, update and update servers.	No	Yes
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 (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 Types**

<b>Log File Type</b>	<b>Description</b>	<b>Supports Syslog Push?</b>	<b>Enabled by Default?</b>
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.  <b>Note:</b> 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 (System Health Daemon)	Records a history of the health of system services and a history of unexpected daemon restarts.	Yes	Yes
SNMP Logs	Records debug messages related to the SNMP network management engine.	Yes	Yes
SNMP Module Logs	Records Web Proxy messages related to interacting with the SNMP monitoring system.	No	No
Sophos Integration Framework Logs	Records messages related to communication between the Web Proxy and the Sophos scanning engine.	No	No
Sophos Logs	Records the status of anti-malware scanning activity from the Sophos scanning engine.	Yes	Yes
Status Logs	Records information related to the system, such as feature key downloads.	Yes	Yes
System Logs	Records DNS, error, and commit activity.	Yes	Yes
Traffic Monitor Error Logs	Records L4TM interface and capture errors.	Yes	Yes
Traffic Monitor Logs	Records sites added to the L4TM block and allow lists.	No	Yes
UDS Logs (User Discovery Service)	Records data about how the Web Proxy discovers the user name without doing actual authentication. It includes information about interacting with the Cisco adaptive security appliance for the Secure Mobility as well as integrating with the Novell eDirectory server for transparent user identification.	Yes	Yes
Updater Logs	Records a history of WBRS and other updates.	Yes	Yes
W3C Logs	Records Web Proxy client history in a W3C compliant format.  For more information, see <a href="#">W3C Compliant Access Log Files, page 11-24</a> .	Yes	No
WBNP Logs (SensorBase Network Participation)	Records a history of Cisco SensorBase Network participation uploads to the SensorBase network.	No	Yes

Log File Type	Description	Supports Syslog Push?	Enabled by Default?
WBRS Framework Logs (Web Reputation Score)	Records messages related to communication between the Web Proxy and the Web Reputation Filters.	No	No
WCCP Module Logs	Records Web Proxy messages related to implementing WCCP.	No	No
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.

**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.  <b>Note</b> 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.

Option	Description
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	<p>The maximum time interval before the current log file is archived and a new log file started. The following interval types are available:</p> <ul style="list-style-type: none"> <li>• <b>None.</b> AsyncOS only performs a rollover when the log file reaches the maximum file size.</li> <li>• <b>Custom Time Interval.</b> 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.</li> <li>• <b>Daily Rollover.</b> 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.</li> <li>• <b>Weekly Rollover.</b> AsyncOS performs a rollover on one or more days of the week at a specified time.</li> </ul>
Log Style (Access Logs)	Specifies the log format to use, either Squid, Apache, or Squid Details.
Custom Fields (Access Logs)	<p>Allows you to include custom information in each access log entry.</p> <p>The syntax for entering format specifiers in the Custom Field is as follows:</p> <pre>&lt;formatSpecifier_1&gt; &lt;formatSpecifier_2&gt; ...</pre> <p>For example: %a %b %E</p> <p>You can add tokens before the format specifiers to display descriptive text in the access log file. For example:</p> <pre>client_IP %a body_bytes %b error_type %E</pre> <p>where client_IP is the description token for log format specifier %a, and so on.</p>
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.

Option	Description
Log Fields  (W3C Access Logs)	<p>Allows you to choose the fields you want to include in the W3C access log. Select a field in the Available Fields list, or type a field in the Custom Field box, and click <b>Add</b>.</p> <p>The order the fields appear in the Selected Log Fields list determines the order of fields in the W3C access log file. You can change the order of fields using the <b>Move Up</b> and <b>Move Down</b> buttons. You can remove a field by selecting it in the Selected Log Fields list and clicking <b>Remove</b>.</p> <p>You can enter multiple user defined fields in the Custom Fields box and add them simultaneously as long as each entry is separated by a new line (click Enter) before clicking <b>Add</b>.</p> <p>When you change the log fields included in a W3C log subscription, the log subscription automatically rolls over. This allows the latest version of the log file to include the correct new field headers.</p>
Log Compression	Specifies whether or not rolled over files are compressed. AsyncOS compresses log files using the gzip compression format.
Log Exclusions  (Optional)  (Access Logs)	<p>Allows you to specify HTTP status codes (4xx or 5xx only) to exclude the associated transactions from an access log or a W3C access log.</p> <p>For example, entering 401 will filter out authentication failure requests that have that transaction number.</p>
Log Level	<p>Specifies the level of detail for log entries. Choose from:</p> <ul style="list-style-type: none"> <li>• <b>Critical.</b> Includes errors only. This is the least detailed setting and is equivalent to the syslog level “Alert.”</li> <li>• <b>Warning.</b> Includes errors and warnings. This log level is equivalent to the syslog level “Warning.”</li> <li>• <b>Information.</b> Includes errors, warnings and additional system operations. This is the default detail level and is equivalent to the syslog level “Info.”</li> <li>• <b>Debug.</b> 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.”</li> <li>• <b>Trace.</b> 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.”</li> </ul> <p><b>Note</b> More detailed settings create larger log files and have a greater impact on system performance.</p>
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.

Option	Description
Retrieval Method: FTP on Appliance	<p>The FTP on Appliance method (equivalent to FTP Poll) requires a remote FTP client accessing the appliance to retrieve log files using an admin or operator user's username and passphrase.</p> <p>When you choose this method, you must enter the maximum number of log files to store on the appliance. When the maximum number is reached, the system deletes the oldest file.</p> <p>This is the default retrieval method.</p>
Retrieval Method: FTP on Remote Server	<p>The FTP on Remote Server method (equivalent to FTP Push) periodically pushes log files to an FTP server on a remote computer.</p> <p>When you choose this method, you must enter the following information:</p> <ul style="list-style-type: none"> <li>• FTP server hostname</li> <li>• Directory on FTP server to store the log file</li> <li>• Username and passphrase of a user that has permission to connect to the FTP server</li> </ul> <p><b>Note</b> AsyncOS for Web only supports passive mode for remote FTP servers. It cannot push log files to an FTP server in active mode.</p>
Retrieval Method: SCP on Remote Server	<p>The SCP on Remote Server method (equivalent to SCP Push) periodically pushes log files using the secure copy protocol to a remote SCP server. This method requires an SSH SCP server on a remote computer using the SSH2 protocol. The subscription requires a user name, SSH key, and destination directory on the remote computer. Log files are transferred based on a rollover schedule set by you.</p> <p>When you choose this method, you must enter the following information:</p> <ul style="list-style-type: none"> <li>• SCP server hostname</li> <li>• Directory on SCP server to store the log file</li> <li>• Username of a user that has permission to connect to the SCP server</li> </ul>
Retrieval Method: Syslog Push	<p>You can only choose syslog for text-based logs.</p> <p>The Syslog Push method sends log messages to a remote syslog server on port 514. This method conforms to RFC 3164.</p> <p>When you choose this method, you must enter the following information:</p> <ul style="list-style-type: none"> <li>• Syslog server hostname</li> <li>• Protocol to use for transmission, either UDP or TCP</li> <li>• Maximum message size</li> </ul> <p>Valid values for UDP are 1024 to 9216.  Valid values for TCP are 1024 to 65535.  Maximum message size depends on the syslog server configuration.</p> <ul style="list-style-type: none"> <li>• Facility to use with the log</li> </ul>

**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, page 11-11](#).

**Related Topics**

- [Log File Types, page 11-3](#)
- [Log File Names and Appliance Directory Structure, page 11-12](#)

# 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, page 11-7](#)

**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.

- e. 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 File Names and Appliance Directory Structure**

- Log Compression
- Retrieval Method

You can also manually archive (rollover) log files.

---

**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.

---

**Related Topics**

- [Adding and Editing Log Subscriptions, page 11-7](#)
- [Log File Names and Appliance Directory Structure, page 11-12](#)

## 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, page 11-13](#).
- [Web Proxy Information in Access Log Files, page 11-13](#).

- Interpreting W3C Access Logs, page 11-24.
- Interpreting Traffic Monitor Logs, page 11-29.
- Log File Fields and Tags, page 11-30.

## 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.

**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.

### Related Topics

- [Web Proxy Information in Access Log Files, page 11-13.](#)
- [Interpreting W3C Access Logs, page 11-24.](#)
- [Interpreting Traffic Monitor Logs, page 11-29.](#)

## 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  
<IW_comp, 6.9, -, "-", "-", "-", "-", "-", "-", "-", "-", IW_comp, -, "-", "-", "-", "Unknown", "Unknown", "-", "-", 198.34, 0, -, [Local], "-", 37, "W32.CiscoTestVector", 33, 0, "WSA-INFECTED-FILE.p  
df", "fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"> -
```

## ■ Web Proxy Information in Access Log Files

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	<p>Client IP address.</p> <p><b>Note:</b> You can choose to mask the IP address in the access logs using the <code>advancedproxyconfig &gt; authentication</code> CLI command.</p>
%w	TCP_MISS	<p>Transaction result code.</p> <p>For more information, see <a href="#">W3C Compliant Access Log Files, page 11-24</a>.</p>
%h	200	HTTP response code.
%s	8187	Response size (headers + body).
%2r	GET http://my.site.com/	<p>First line of the request.</p> <p><b>Note:</b> 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.</p> <p>The following characters are URL encoded:</p> <p>&amp; # % + , : ; = @ ^ { } [ ]</p>
%A	-	<p>Authenticated username.</p> <p><b>Note:</b> You can choose to mask the username in the access logs using the <code>advancedproxyconfig &gt; authentication</code> CLI command.</p>
%H	DIRECT	<p>Code that describes which server was contacted for the retrieving the request content.</p> <p>Most common values include:</p> <ul style="list-style-type: none"> <li>• <b>NONE.</b> The Web Proxy had the content, so it did not contact any other server to retrieve the content.</li> <li>• <b>DIRECT.</b> The Web Proxy went to the server named in the request to get the content.</li> <li>• <b>DEFAULT_PARENT.</b> The Web Proxy went to its primary parent proxy or an external DLP server to get the content.</li> </ul>
%d	my.site.com	Data source or server IP address.
%c	text/plain	Response body MIME type.
%D	DEFAULT_CASE_11	<p>ACL decision tag.</p> <p><b>Note:</b> The end of the ACL decision tag includes a dynamically generated number that the Web Proxy uses internally. You can ignore this number.</p> <p>For more information, see <a href="#">ACL Decision Tags, page 11-16</a>.</p>

Format Specifier	Field Value	Field Description
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.” 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. Any space in the policy group name is replaced with an underscore ( _ ).
N/A (Part of the ACL decision tag)	OutboundMalwareScanningPolicy	Outbound Malware Scanning Policy group name. Any space in the policy group name is replaced with an underscore ( _ ).
N/A (Part of the ACL decision tag)	DataSecurityPolicy	Cisco IronPort Data Security Policy group name. When the transaction matches the global Cisco IronPort Data Security Policy, this value is “DefaultGroup.” This policy group name only appears when Cisco IronPort Data Security Filters is enabled. “NONE” appears when no Data Security Policy was applied. 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. 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 <i>ProxyGroupName/ProxyServerName</i> . When the transaction matches the global Routing Policy, this value is “DefaultRouting.” When no upstream proxy server is used, this value is “DIRECT.” Any space in the policy group name is replaced with an underscore ( _ ).
%Xr	<IW_comp, 6.9,-,"-", -, -, -, -, -, -,"- ", -, -, -, "-", -, -, "Unknown", "Unknown", "- ", "-", 198.34,0, -, [Local], "-", 37, "W32.CiscoTestVector", 33,0, "WSA-INFECTED-FILE.pdf", "fd5ef49d4213e05f448f11ed9c98253d85829614fb368a421d14e64c426da5e">	Scanning verdict information. Inside the angled brackets, the access logs include verdict information from various scanning engines. For more information about the values included within the angled brackets, see <a href="#">Interpreting Access Log Scanning Verdict Entries, page 11-20</a> and <a href="#">Malware Scanning Verdict Values, page 11-40</a> .
">%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
<code>TCP_HIT</code>	The object requested was fetched from the disk cache.
<code>TCP_IMS_HIT</code>	The client sent an IMS (If-Modified-Since) request for an object and the object was found in the cache. The proxy responds with a 304 response.
<code>TCP_MEM_HIT</code>	The object requested was fetched from the memory cache.
<code>TCP_MISS</code>	The object was not found in the cache, so it was fetched from the origin server.
<code>TCP_REFRESH_HIT</code>	The object was in the cache, but had expired. The proxy sent an IMS (If-Modified-Since) request to the origin server, and the server confirmed that the object has not been modified. Therefore, the appliance fetched the object from either the disk or memory cache.
<code>TCP_CLIENT_REFRESH_MISS</code>	The client sent a “don’t fetch response from cache” request by issuing the ‘Pragma: no-cache’ header. Due to this header from the client, the appliance fetched the object from the origin server.
<code>TCP_DENIED</code>	The client request was denied due to Access Policies.
<code>UDP_MISS</code>	The object was fetched from the origin server.
<code>NONE</code>	There was an error in the transaction. For example, a DNS failure or gateway timeout.

## 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
<code>ALLOW_ADMIN_ERROR_PAGE</code>	The Web Proxy allowed the transaction to an notification page and to any logo used on that page.
<code>ALLOW_CUSTOMCAT</code>	The Web Proxy allowed the transaction based on custom URL category filtering settings for the Access Policy group.
<code>ALLOW_REFERER</code>	The Web Proxy allowed the transaction based on an embedded/referred content exemption.
<code>ALLOW_WBRS</code>	The Web Proxy allowed the transaction based on the Web Reputation filter settings for the Access Policy group.

<b>ACL Decision Tag</b>	<b>Description</b>
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.
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 WSA itself, only requests to the actual WSA 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_AVG	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.”

## Web Proxy Information in Access Log Files

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.
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_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.
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.
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.

<b>ACL Decision Tag</b>	<b>Description</b>
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_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.

ACL Decision Tag	Description
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:



## Note

For an example of a whole access log file entry, see [Web Proxy Information in Access Log Files, page 11-13](#).

Each element in this example corresponds to a log-file format specifier as shown in the following table:

<b>Position</b>	<b>Field Value</b>	<b>Format Specifier</b>	<b>Description</b>
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	<p>The malware scanning verdict Webroot passed to the DVS engine. Applies to responses detected by Webroot only.</p> <p>For more information, see <a href="#">Malware Scanning Verdict Values, page 11-40</a>.</p>

<b>Position</b>	<b>Field Value</b>	<b>FormatSpecifier</b>	<b>Description</b>
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.
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. For more information, see <a href="#">Malware Scanning Verdict Values, page 11-40</a> .
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. For more information, see <a href="#">Malware Scanning Verdict Values, page 11-40</a> .
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.
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.

## Web Proxy Information in Access Log Files

Position	Field Value	FormatSpecifier	Description
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: <ul style="list-style-type: none"> <li>• <b>0.</b> Allow</li> <li>• <b>1.</b> Block</li> <li>• <b>- (hyphen).</b> 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.</li> </ul>
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: <ul style="list-style-type: none"> <li>• <b>0.</b> Allow</li> <li>• <b>1.</b> Block</li> <li>• <b>- (hyphen).</b> 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 &gt; Destinations page.</li> </ul>
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. For a list of URL category abbreviations, see <a href="#">URL Category Descriptions, page 9-25</a> .
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). For a list of URL category abbreviations, see <a href="#">URL Category Descriptions, page 9-25</a> .
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 threat type returned by the Web Reputation filters which resulted in the target website receiving a poor reputation. Typically, this field is populated for sites at reputation of -4 and below.
24	"Unknown"	"%XO"	The application name as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled.
25	"Unknown"	"%Xu"	The application type as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled.
26	"-"	"%Xb"	The application behavior as returned by the AVC engine, if applicable. Only applies when the AVC engine is enabled.

Position	Field Value	FormatSpecifier	Description
27	" - "	"%XS"	<p>Safe browsing scanning verdict. This value indicates whether either the safe search or the site content ratings feature was applied to the transaction.</p> <p>For a list of the possible values, see <a href="#">Logging Adult Content Access, page 9-18</a>.</p>
28	489.73	%XB	The average bandwidth consumed serving the request, in Kb/sec.
29	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.
30	[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 (-).
31	" - "	"%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.
32	" - "	"%X4"	<p>The threat name assigned to the client request that was blocked or monitored due to an applicable Outbound Malware Scanning Policy.</p> <p>This threat name is independent of which anti-malware scanning engines are enabled.</p>
33	37	%X#1#	<p>Verdict from Advanced Malware Protection file scanning:</p> <ul style="list-style-type: none"> <li>• 0: File is not malicious</li> <li>• 1: File was not scanned because of its file type</li> <li>• 2: File scan timed out</li> <li>• 3: Scan error</li> <li>• Greater than 3: File is malicious</li> </ul>
34	"W32.CiscoTestVector"	%X#2#	Threat name, as determined by Advanced Malware Protection file scanning; "-" indicates no threat.
35	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.
36	0	%X#4#	<p>Indicator of upload and analysis request:</p> <p>"0" indicates that Advanced Malware Protection did not request upload of the file for analysis.</p> <p>"1" indicates that Advanced Malware Protection did request upload of the file for analysis.</p>

## ■ W3C Compliant Access Log Files

Position	Field Value	Format Specifier	Description
37	"WSA-INFECTED-FILE.pdf"	%X#5#	The name of the file being downloaded and analyzed.
38	"fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e	%X#6#	The SHA-256 identifier for this file.

Refer to [Log File Fields and Tags, page 11-30](#) for a description of each format specifier's function.

### Related Topics

- [Web Proxy Information in Access Log Files, page 11-13](#)
- [Customizing Access Logs, page 11-26](#).
- [W3C Compliant Access Log Files, page 11-24](#)
- [Viewing Log Files, page 11-13](#)
- [Log File Fields and Tags, page 11-30](#)

## 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, page 11-24](#)
- [Interpreting W3C Access Logs, page 11-24](#)

## W3C Field Types

When defining a W3C access log subscription, you must choose which log fields to include, such as the ACL decision tag or the client IP address. You can include one of the following types of log fields:

- **Predefined.** The web interface includes a list of fields from which you can choose.
- **User defined.** You can type a log field that is not included in the predefined list.

## Interpreting W3C Access Logs

Consider the following rules and guidelines when interpreting W3C access logs:

- Administrators decide what data is recorded in each W3C access log subscription; therefore, W3C access logs have no set field format.
- W3C logs are self-describing. The file format (list of fields) is defined in a header at the start of each log file.
- Fields in the W3C access logs are separated by a white space.
- If a field contains no data for a particular entry, a hyphen ( - ) is included in the log file instead.

- Each line in the W3C access log file relates to one transaction, and each line is terminated by a LF sequence.
- [W3C Log File Headers, page 11-25](#)
- [W3C Field Prefixes, page 11-25](#)

## 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.

## ■ Customizing Access Logs

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, page 11-13.](#)
- [Customizing Access Logs, page 11-26.](#)
- [Traffic Monitor Log Files, page 11-29.](#)
- [Log File Fields and Tags, page 11-30.](#)
- [Viewing Log Files, page 11-13.](#)

## Customizing Access Logs

You can customize regular and W3C access logs to include many different fields to capture comprehensive information about web traffic within the network using predefined fields or user defined fields.

### Related Topics

- For a list of predefined fields, see [Log File Fields and Tags, page 11-30.](#)
- For information on user defined fields, see [Access Log User Defined Fields, page 11-26.](#)

## 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:

<b>Header Type</b>	<b>Access Log Format Specifier Syntax</b>	<b>W3C Log Custom Field Syntax</b>
Header from the client application	<code>%&lt;ClientHeaderName:</code>	<code>cs(ClientHeaderName)</code>
Header from the server	<code>%&lt;ServerHeaderName:</code>	<code>sc(ServerHeaderName)</code>

For example, if you want to log the If-Modified-Since header value in client requests, enter the following text in the Custom Fields box for a W3C log subscription:

```
cs(If-Modified-Since)
```

### Related Topics

- [Customizing Regular Access Logs, page 11-27.](#)
- [Customizing W3C Access Logs, page 11-27.](#)

## Customizing Regular Access Logs

- 
- Step 1** Choose System Administration > Log Subscriptions.
- Step 2** Click the access log file name to edit the access log subscription.
- Step 3** Enter the required format specifiers in the Custom Field.

The syntax for entering format specifiers in the Custom Field is as follows:

```
<formatSpecifier_1> <formatSpecifier_2> ...
```

For example: %a %b %E

You can add tokens before the format specifiers to display descriptive text in the access log file.  
For example:

```
client_IP %a body_bytes %b error_type %E
```

where client\_IP is the description token for log format specifier %a, and so on.



**Note** You can create a custom field for any header in a client request or a server response.

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

### Related Topics

- [Web Proxy Information in Access Log Files, page 11-13.](#)
- [Log File Fields and Tags, page 11-30.](#)
- [Access Log User Defined Fields, page 11-26.](#)

## Customizing W3C Access Logs

- 
- Step 1** Choose System Administration > Log Subscriptions
- Step 2** Click the W3C log file name to edit the W3C log subscription.
- Step 3** Type a field in the Custom Field box, and click **Add**.

The order the fields appear in the Selected Log Fields list determines the order of fields in the W3C access log file. You can change the order of fields using the **Move Up** and **Move Down** buttons. You can remove a field by selecting it in the Selected Log Fields list and clicking **Remove**.

You can enter multiple user defined fields in the Custom Fields box and add them simultaneously as long as each entry is separated by a new line (click Enter) before clicking **Add**.

When you change the log fields included in a W3C log subscription, the log subscription automatically rolls over. This allows the latest version of the log file to include the correct new field headers.



**Note** You can create a custom field for any header in a client request or a server response.

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

**Related Topics**

- [W3C Compliant Access Log Files, page 11-24.](#)
- [Log File Fields and Tags, page 11-30.](#)
- [Access Log User Defined Fields, page 11-26.](#)
- [Configuring CTA-specific Custom W3C Logs, page 11-28.](#)

## Configuring CTA-specific Custom W3C Logs

You can configure the WSA to “push” Cognitive Threat Analytics (CTA)-specific custom W3C access logs to Cisco’s Cloud Web Security service for analysis and reporting. Cisco ScanCenter is the administration portal into Cloud Web Security (CWS).

**Before You Begin**

- Create a device account in Cisco ScanCenter for your WSA, selecting **SCP** as the automatic upload protocol (see the “Proxy Device Uploads” section of the *Cisco ScanCenter Administrator Guide* for more information). Note the SCP (Secure Copy Protocol) host name and the generated user name for your WSA (case sensitive, different for each device).

---

**Step 1** Follow the instructions in [Customizing W3C Access Logs, page 11-27](#) to add a new W3C access log subscription, choosing **W3C Logs** as the **Log Type**.

**Step 2** Provide a descriptive **Log Name**.

**Step 3** Delete any entries in the **Selected Log Fields** list (select all and click **Remove**).

**Step 4** Add the following fields to the **Selected Log Fields** list:

- a. Copy and paste the following into the **Custom Fields** box and then click **Add**.

```
timestamp
xelapsed-time
c-ip
cs-username
c-port
s-ip
s-port
cs-url
cs-bytes
sc-bytes
cs(User-Agent)
cs-mime-type
cs-method
sc-http-status
cs(Referer)
sc(Location)
x-amp-sha
x-amp-verdict
x-amp-malware-name
x-amp-score
```

**Step 5** Provide a **Rollover by File Size**; in this case, 500M is recommended.

**Step 6** Choose a **Rollover by Time** option.

We recommend a **Custom Time Interval**, with a **Rollover every:** time interval based on these guidelines:

Number of Users Behind Proxy	Recommended Rollover Period
Unknown or less than 2000	55 minutes
2000 to 4000	30 minutes
4000 to 6000	20 minutes
More than 6000	10 minutes

**Step 7** For the **Retrieval Method**, select **SCP on Remote Server** and enter the CTA server information from your CWS account.

- a. In the **SCP Host** field, enter the SCP host provided in Cisco ScanCenter; for example, `etr.cloudsec.sco.cisco.com`.
- b. In the **SCP Port** field, enter `22`.
- c. In the **Directory** field, enter `/upload`.
- d. In the **Username** field, enter the user name generated for your device in Cisco ScanCenter. The device user name is case sensitive and different for each proxy device.
- e. Check **Enable Host Key Checking**, and select **Automatically Scan**.

**Step 8** Click **Submit** on the WSA.

A public SSH key is generated by the WSA and displayed in the Management Console.

**Step 9** Copy the public SSH key generated by the WSA to the Clipboard.

**Step 10** Switch to the Cisco ScanCenter portal, select the appropriate device account and then paste the public SSH key into the CTA Device Provisioning page. (See the “Proxy Device Uploads” section of the *Cisco ScanCenter Administrator Guide* for additional information.)

Successful authentication between your proxy device and CTA system will allow log files from your proxy device to be uploaded to the CTA system for analysis.

Cisco’s ScanCenter is the administration portal to Cisco Cloud Web Security. See <http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html>.

**Step 11** Switch back to the WSA, and click **Commit Changes**.

**Note** The WSA restarts when committing configuration changes, so connected users may be temporarily disconnected.

## Traffic Monitor Log Files

Layer-4 Traffic Monitor log files provides a detailed record of Layer-4 monitoring activity. You can view Layer-4 Traffic Monitor log file entries to track updates to firewall block lists and firewall allow lists.

## Interpreting Traffic Monitor Logs

Use the examples below to interpret the various entry types contains in Traffic Monitor Logs.

**Example 1**

172.xx.xx.xx discovered for blocksite.net (blocksite.net) added to firewall block list.

In this example, where a match becomes a block list firewall entry. The Layer-4 Traffic Monitor matched an IP address to a domain name in the block list based on a DNS request which passed through the appliance. The IP address is then entered into the block list for the firewall.

**Example 2**

172.xx.xx.xx discovered for www.allowsite.com (www.allowsite.com) added to firewall allow list.

In this example, a match becomes an allow list firewall entry. The Layer-4 Traffic Monitor matched a domain name entry and added it to the appliance allow list. The IP address is then entered into the allow list for the firewall.

**Example 3**

Firewall noted data from 172.xx.xx.xx to 209.xx.xx.xx (allowsite.net):80.

In this example, the Layer-4 Traffic Monitor logs a record of data that passed between an internal IP address and an external IP address which is on the block list. Also, the Layer-4 Traffic Monitor is set to monitor, not block.

**Related Topics**

- [Viewing Log Files, page 11-13](#)

## Log File Fields and Tags

- [Access Log Format Specifiers and W3C Log File Fields, page 11-30](#)
- [Transaction Result Codes, page 11-16](#)
- [ACL Decision Tags, page 11-16](#)
- [Malware Scanning Verdict Values, page 11-40](#)

## 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, page 11-26](#) and information about custom fields in [Adding and Editing Log Subscriptions, page 11-7](#).

The following table describes these variables:

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%:<1	x-p2s-first-byte-time	The time it takes from the moment the Web Proxy starts connecting to the server to the time it is first able to write to the server. If the Web Proxy has to connect to several servers to complete the transaction, it is the sum of those times.
%:<a	x-p2p-auth-wait-time	Wait-time to receive the response from the Web Proxy authentication process, after the Web Proxy sent the request.
%:<b	x-p2s-body-time	Wait-time to write request body to server after header.
%:<d	x-p2p-dns-wait-time	Time taken by the Web Proxy to send the DNS request to the Web Proxy DNS process.
%:<h	x-p2s-header-time	Wait-time to write request header to server after first byte.
%:<r	x-p2p-reputation-wait-time	Wait-time to receive the response from the Web Reputation Filters, after the Web Proxy sent the request.
%:<s	x-p2p-asw-req-wait-time	Wait-time to receive the verdict from the Web Proxy anti-spyware process, after the Web Proxy sent the request.
%:>1	x-s2p-first-byte-time	Wait-time for first response byte from server
%:>a	x-p2p-auth-svc-time	Wait-time to receive the response from the Web Proxy authentication process, including the time required for the Web Proxy to send the request.
%:>b	x-s2p-body-time	Wait-time for complete response body after header received
%:>c	x-p2p-fetch-time	Time required for the Web Proxy to read a response from the disk cache.
%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy DNS process to send back a DNS result to the Web Proxy.
%:>h	x-s2p-header-time	Wait-time for server header after first response byte
%:>r	x-p2p-reputation-svc-time	Wait-time to receive the verdict from the Web Reputation Filters, including the time required for the Web Proxy to send the request.
%:>s	x-p2p-asw-req-svc-time	Wait-time to receive the verdict from the Web Proxy anti-spyware process, including the time required for the Web Proxy to send the request.
%:1<	x-c2p-first-byte-time	Wait-time for first request byte from new client connection.
%:1>	x-p2c-first-byte-time	Wait-time for first byte written to client.
%:A<	x-p2p-avc-svc-time	Wait-time to receive the response from the AVC process, including the time required for the Web Proxy to send the request.

## ■ Log File Fields and Tags

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%: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-s2p-header-time	Wait-time for complete header written to client
%:m<	x-p2p-mcafee-resp-svc-time	Wait-time to receive the verdict from the McAfee scanning engine, including the time required for the Web Proxy to send the request.
%:m>	x-p2p-mcafee-resp-wait-time	Wait-time to receive the response from the McAfee scanning engine, after the Web Proxy sent the request.
%:p<	x-p2p-sophos-resp-svc-time	Wait-time to receive the verdict from the Sophos scanning engine, including the time required for the Web Proxy to send the request.
%:p>	x-p2p-sophos-resp-wait-time	Wait-time to receive the response from the Sophos scanning engine, after the Web Proxy sent the request.
%:w<	x-p2p-webroot-resp-svc-time	Wait-time to receive the verdict from the Webroot scanning engine, including the time required for the Web Proxy to send the request.
%:w>	x-p2p-webroot-resp-wait-time	Wait-time to receive the response from the Webroot scanning engine, after the Web Proxy sent the request.
%?BLOCK_SUSPECT_USER_AGE_NT_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).

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%c	cs-mime-type	Response body MIME type. This field is written with double-quotes in the access logs.
%C	cs(Cookie)	Cookie header. This field is written with double-quotes in the access logs.
%d	s-hostname	Data source or server IP address.
%D	x-acltag	ACL decision tag.
%e	x-elapsed-time	Elapsed time in milliseconds. For TCP traffic, this is the time elapsed between the opening and closing of the HTTP connection. 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. This field is used for troubleshooting policy/authentication issues to determine whether a user is matching the correct group or policy.
%h	sc-http-status	HTTP response code.
%H	s-hierarchy	Hierarchy retrieval.
%i	x-icap-server	IP address of the last ICAP server contacted while processing the request.
%I	x-transaction-id	Transaction ID.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%j	DCF	<p>Do not cache response code; DCF flags.</p> <p>Response code descriptions:</p> <ul style="list-style-type: none"> <li>• Response code based on client request: <ul style="list-style-type: none"> <li>– 1 = Request had “no-cache” header.</li> <li>– 2 = Caching is not authorized for the request.</li> <li>– 4 = Request is missing the 'Variant' header.</li> <li>– 8 = Username or passphrase needed for user request.</li> <li>– 20 = Response for specified HTTP method.</li> </ul> </li> <li>• Response code based on response received by the appliance: <ul style="list-style-type: none"> <li>– 40 = Response contains “Cache-Control: private” header.</li> <li>– 80 = Response contains “Cache-Control: no-store” header.</li> <li>– 100 = Response indicates that request was a query.</li> <li>– 200 = Response has a small “Expires” value (expires soon).</li> <li>– 400 = Response does not have “Last Modified” header.</li> <li>– 1000 = Response expires immediately.</li> <li>– 2000 = Response file is too big to cache.</li> <li>– 20000 = New copy of file exists.</li> <li>– 40000 = Response has bad/invalid values in “Vary” header.</li> <li>– 80000 = Response requires setting of cookies.</li> <li>– 100000 = Non-cacheable HTTP STATUS Code.</li> <li>– 200000 = Object received by appliance was incomplete (based on size).</li> <li>– 800000 = Response trailers indicate no caching.</li> <li>– 1000000 = Response requires re-write.</li> </ul> </li> </ul>
%k	s-ip	<p>Data source IP address (server IP address)</p> <p>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.</p>
%1	user-type	Type of user, either local or remote.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%L	x-local_time	<p>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.</p> <p>Enabling this field allows you to correlate logs to issues without having to calculate local time from epoch time for each log entry.</p>
%m	cs-auth-mechanism	<p>Used to troubleshoot authentication issues.</p> <p>The authentication mechanism used on the transaction. Possible values are:</p> <ul style="list-style-type: none"> <li>• <b>BASIC.</b> The user name was authenticated using the Basic authentication scheme.</li> <li>• <b>NTLMSSP.</b> The user name was authenticated using the NTLMSSP authentication scheme.</li> <li>• <b>Kerberos.</b> The user name was authenticated using the Kerberos authentication scheme.</li> <li>• <b>SSO_TUI.</b> The user name was obtained by matching the client IP address to an authenticated user name using transparent user identification.</li> <li>• <b>SSO_ISE.</b> The user was authenticated by an ISE server. (Log shows GUEST if that is chosen as the fall-back mechanism for ISE authentication.)</li> <li>• <b>SSO ASA.</b> The user is a remote user and the user name was obtained from a Cisco ASA using the Secure Mobility.</li> <li>• <b>FORM_AUTH.</b> The user entered authentication credentials in a form in the web browser when accessing a application.</li> <li>• <b>GUEST.</b> The user failed authentication and instead was granted guest access.</li> </ul>
%M	CMF	Cache miss flags: CMF flags.
%N	s-computerName	Server name or destination hostname. This field is written with double-quotes in the access logs.
%p	s-port	Destination port number.
%P	cs-version	Protocol.
%q	cs-bytes	Request size (headers + body).
%r	x-req-first-line	Request first line - request method, URI.
%s	sc-bytes	Response size (header + body).

## ■ Log File Fields and Tags

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%t	timestamp	<p>Timestamp in UNIX epoch.</p> <p><b>Note:</b> 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.</p>
%u	cs(User-Agent)	<p>User agent. This field is written with double-quotes in the access logs.</p> <p>This field helps determine if an application is failing authentication and/or requires different access permissions.</p>
%U	cs-uri	Request URI.
%v	date	Date in YYYY-MM-DD.
%V	time	Time in HH:MM:SS.
%w	sc-result-code	Result code. For example: TCP_MISS, TCP_HIT.
%W	sc-result-code-denial	Result code denial.
%x	x-latency	Latency.
%X0	x-resp-dvs-scanverdict	<p>Unified response-side anti-malware scanning verdict that provides the <i>malware category number</i> independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning.</p> <p>This field is written with double-quotes in the access logs.</p>
%X1	x-resp-dvs-threat-name	<p>Unified response-side anti-malware scanning verdict that provides the <i>malware threat name</i> independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning.</p> <p>This field is written with double-quotes in the access logs.</p>
%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	<p>Indicates whether Adaptive Scanning blocked the transaction without invoke any anti-malware scanning engine. The possible values are:</p> <ul style="list-style-type: none"> <li>• <b>1.</b> Transaction was blocked.</li> <li>• <b>0.</b> Transaction was not blocked.</li> </ul> <p>This variable is included in the scanning verdict information (in the angled brackets at the end of each access log entry).</p>

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%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).
%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.
%XI	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.

## ■ Log File Fields and Tags

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%XP	x-acl-added-headers	Unrecognized header. Use this field to log extra headers in client requests. This supports troubleshooting of specialized systems that add headers to client requests as a way of authenticating and redirecting those requests, for example, YouTube for Schools.
%XQ	x-webcat-req-code-abbr	The predefined URL category verdict determined during request-side scanning, abbreviated.
%Xr	x-result-code	Scanning verdict information.
%XR	x-webcat-req-code-full	The URL category verdict determined during request-side scanning, full name.
%Xs	x-webroot-spyid	Webroot specific identifier: (Spy ID).
%XS	x-request-rewrite	Safe browsing scanning verdict.  Indicates whether 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-wbtrs-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 <i>malware category</i> independent of which scanning engines are enabled. Applies to transactions blocked or monitored due to server response scanning.  This field is written with double-quotes in the access logs.

Format Specifier in Access Logs	Log Field in W3C Logs	Description
%X#1#	x-amp-verdict	Verdict from Advanced Malware Protection file scanning: <ul style="list-style-type: none"><li>• 0: File is not malicious.</li><li>• 1: File was not scanned because of its file type.</li><li>• 2: File scan timed out.</li><li>• 3: Scan error.</li><li>• Greater than 3: File is malicious.</li></ul>
%X#2#	x-amp-malware-name	Threat name, as determined by Advanced Malware Protection file scanning. “-” indicates no threat.
%X#3#	x-amp-score	Reputation score from Advanced Malware Protection file scanning. This score is used only if the cloud reputation service is unable to determine a clear verdict for the file.
%X#4#	x-amp-upload	Indicator of upload and analysis request: “0” indicates that Advanced Malware Protection did not request upload of the file for analysis. “1” indicates that Advanced Malware Protection did request upload of the file for analysis.
%X#5#	x-amp-filename	The name of the file being downloaded and analyzed.
%X#6#	x-amp-sha	The SHA-256 identifier for this file.
%y	cs-method	Method.
%Y	cs-url	The entire URL.
N/A	x-hierarchy-origin	Code that describes which server was contacted for the retrieving the request content (for example, DIRECT/www.example.com).
N/A	x-resultcode-httpstatus	Result code and the HTTP response code, with a slash (/) in between.

### Related Topics

- [Web Proxy Information in Access Log Files, page 11-13.](#)
- [Interpreting W3C Access Logs, page 11-24.](#)

## 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
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, page 11-13.](#)
- [Interpreting W3C Access Logs, page 11-24.](#)

# Troubleshooting Logging

- Custom URL Categories Not Appearing in Access Log Entries, page A-8
- Logging HTTPS Transactions, page A-8
- Alert: Unable to Maintain the Rate of Data Being Generated, page A-9
- Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs, page A-9

**Troubleshooting Logging**



## Perform System Administration Tasks

---

- [Overview of System Administration, page 12-1](#)
- [Saving, Loading, and Resetting the Appliance Configuration, page 12-2](#)
- [Working with Feature Keys, page 12-3](#)
- [Virtual Appliance License, page 12-4](#)
- [Enabling Remote Power Cycling, page 12-5](#)
- [Administering User Accounts, page 12-6](#)
- [Defining User Preferences, page 12-10](#)
- [Configuring Administrator Settings, page 12-11](#)
- [Managing Alerts, page 12-14](#)
- [SSL Configuration, page 12-22](#)
- [System Date and Time Management, page 12-21](#)
- [Certificate Management, page 12-24](#)
- [AsyncOS for Web Upgrades and Updates, page 12-27](#)
- [Monitoring System Health and Status Using SNMP, page 12-28](#)

## 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, page 12-2](#)
- [Saving the Appliance Configuration File, page 12-2](#)
- [Loading the Appliance Configuration File, page 12-3](#)
- [Resetting the Appliance Configuration to Factory Defaults, page 12-3](#)

## Viewing and Printing the Appliance Configuration

---

**Step 1** Choose **System Administration > Configuration Summary**.

**Step 2** View or print the Configuration Summary page as required.

---

## Saving the Appliance Configuration File

---

**Step 1** Choose **System Administration > Configuration File**.

**Step 2** Complete the Configuration File options.

Option	Description
Choose from these location options: <ul style="list-style-type: none"> <li>• Download file to local computer to view or save</li> <li>• Save file to this appliance (example.com)</li> <li>• Email file to</li> </ul>	Allows you to choose where to save the file to
Mask passphrases in the Configuration Files	If enabled, causes the original, encrypted passphrase to be replaced with “*****” in the exported or saved file. Please note, however, that configuration files with masked passphrases cannot be loaded directly back into AsyncOS for Web.
Choose from these file name options: <ul style="list-style-type: none"> <li>• Use system-generated file name</li> <li>• Use user-defined file name:</li> </ul>	Allows you to choose the configuration file naming method.

---

**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.

**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.

**Step 1**

Choose **System Administration > Configuration File**.

**Step 2**

Choose Load Configuration options and a file to load. 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.

**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**.

## 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, page 12-4
- Changing Feature Key Update Settings, page 12-4

## Displaying and Updating Feature Keys

- 
- Step 1** Choose **System Administration > Feature Keys**.
- Step 2** To refresh the list of pending keys, click **Check for New Keys** to refresh the list of pending keys.
- Step 3** To add a new feature key manually, paste or type the key into the Feature Key field and click **Submit Key**. If the feature key is valid, the feature key is added to the display.
- Step 4** To activate a new feature key from the Pending Activation list, mark its “Select” checkbox and click **Activate Selected Keys**.

You can configure your appliance to automatically download and install new keys as they are issued. In this case, the Pending Activation list will always be empty. You can tell AsyncOS to look for new keys at any time by clicking the **Check for New Keys** button, even if you have disabled the automatic checking via the Feature Key Settings page.

---

## Changing Feature Key Update Settings

The Feature Key Settings page is used to control whether your appliance checks for and downloads new feature keys, and whether or not those keys are automatically activated.

- 
- Step 1** Choose **System Administration > Feature Key Settings**.
- Step 2** Click **Edit Settings**.
- Step 3** Change the Feature Key Settings as required.

Option	Description
Automatic Serving of Feature Keys	Options to automatically check and download feature keys and to automatically activate downloaded feature keys.  Automatic checks are normally performed once a month but this changes to once a day when a feature key is to expire in less than 10 days and once a day after key expiration, for up to one month. After a month, the expired key is no longer included in the list of expiring/expired keys.

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

## Virtual Appliance License

The Cisco Web Security Virtual appliance requires an additional license to run the virtual appliance on a host.

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 for 180 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, page 12-14](#)

## 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

The ability to remotely reset the power for the appliance chassis is available only on 80-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.

**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, page C-2](#).
- 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 [Appendix B, “Command Line Interface.”](#)

---

**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.

---

#### Related Topics

- [Hardware Appliances: Remotely Resetting Appliance Power, page A-12](#)

## Administering User Accounts

The following types of users can log into the Web Security appliance to manage the appliance:

- **Local users.** You can define users locally on the appliance itself.
- **Users defined in an external system.** You can configure the appliance to connect to an external RADIUS server to authenticate users logging into the appliance.



**Note** Any user you define can log into the appliance using any method, such as logging into the web interface or using SSH.

---

#### Related Topics

- [Managing Local User Accounts, page 12-6.](#)
- [RADIUS User Authentication, page 12-8.](#)

## 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.

---

## Adding Local User Accounts

### Before You Begin

Define the passphrase requirements that all user accounts must follow. See [Setting Passphrase Requirements for Administrative Users, page 12-11](#).

**Step 1** Choose **System Administration > Users**.

**Step 2** Click **Add User**.

**Step 3** Enter a username, noting the following rules:

- Usernames can contain lowercase letters, numbers, and the dash ( - ) character, but cannot begin with a dash.
- Usernames cannot greater than 16 characters.
- Usernames cannot be special names that are reserved by the system, such as “operator” or “root.”
- If you also use external authentication, usernames should not duplicate externally-authenticated usernames.

**Step 4** Enter a full name for the user.

**Step 5** Select a user type.

User Type	Description
Administrator	Allows full access to all system configuration settings. However, the <code>upgradecheck</code> and <code>upgradeinstall</code> CLI commands can be issued only from the system defined “admin” account.
Operator	Restricts users from creating, editing, or removing user accounts. The operators group also restricts the use of the following CLI commands: <ul style="list-style-type: none"><li>• <code>resetconfig</code></li><li>• <code>upgradecheck</code></li><li>• <code>upgradeinstall</code></li><li>• <code>systemsetup</code> or running the System Setup Wizard</li></ul>
Read-Only Operator	User accounts with this role: <ul style="list-style-type: none"><li>• Can view configuration information.</li><li>• Can make and submit changes to see how to configure a feature, but they cannot commit them.</li><li>• Cannot make any other changes to the appliance, such as clearing the cache or saving files.</li><li>• Cannot access the file system, FTP, or SCP.</li></ul>
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

- 
- Step 1** Choose **System Administration > Users**.
- Step 2** Click the trash can icon corresponding to the listed user name and confirm when prompted.
- Step 3** Submit and commit your changes.
- 

## Editing User Accounts

- 
- Step 1** Choose **System Administration > Users**.
- Step 2** Click the user name.
- Step 3** Make changes to the user on the Edit User page as required.
- Step 4** Submit and commit your changes.
- 

## Changing 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, page 12-8](#)
- [Setting Passphrase Requirements for Administrative Users, page 12-11](#)

## 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

- 
- 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 3–5 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.

---

**Defining User Preferences**

- 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.	<p>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.</p> <p>AsyncOS assigns RADIUS users to appliance roles based on the RADIUS CLASS attribute. CLASS attribute requirements:</p> <ul style="list-style-type: none"> <li>• three-character minimum</li> <li>• 253-character maximum</li> <li>• no colons, commas, or newline characters</li> <li>• one or more mapped CLASS attributes for each RADIUS user (With this setting, AsyncOS denies access to RADIUS users without a mapped CLASS attribute.)</li> </ul> <p>For RADIUS users with multiple CLASS attributes, AsyncOS assigns the most restrictive role. For example, if a RADIUS user has two CLASS attributes, which are mapped to the Operator and Read-Only Operator roles, AsyncOS assigns the RADIUS user to the Read-Only Operator role, which is more restrictive than the Operator role.</p> <p>These are the appliance roles ordered from most restrictive to least restrictive:</p> <ul style="list-style-type: none"> <li>• Administrator</li> <li>• Operator</li> <li>• Read-Only Operator</li> <li>• Guest</li> </ul>
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.

**Related Topics**

- [External Authentication, page 5-11](#)
- [Adding Local User Accounts, page 12-7.](#)

## Defining User Preferences

Preference settings, such as reporting display formats, are stored for each user and are the same regardless from which client machine the user logs into the appliance.

- 
- Step 1** Choose Options > Preferences.

**Step 2** On the User Preferences page, click **Edit Preferences**.

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

Preference Setting	Description
Language Display	The language AsyncOS for Web uses in the web interface and CLI.
Landing Page	The page that displays when the user logs into the appliance.
Reporting Time Range Displayed (default)	The default time range that displays for reports on the Reporting tab.
Number of Reporting Rows Displayed	The number of rows of data shown for each report by default.

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

## Configuring Administrator Settings

### Setting Passphrase Requirements for Administrative Users

To set passphrase requirements for locally-defined administrative users of the appliance:

**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.
Passphrase Strength	<p>You can display a passphrase-strength indicator when an administrative user enters a new passphrase.</p> <p>This setting does not enforce creation of strong passphrases, it merely shows how easy it is to guess the entered passphrase.</p> <p>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."</p> <p>Experiment to see what number best meets your requirements.</p> <p>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, Appendix A.</p> <p>Generally, stronger passphrases:</p> <ul style="list-style-type: none"> <li>• Are longer</li> <li>• Include upper case, lower case, numeric, and special characters</li> <li>• Do not include words in any dictionary in any language.</li> </ul> <p>To enforce passphrases with these characteristics, use the other settings on this page.</p>

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

---

## Additional Security Settings for Accessing the Appliance

You can configure the Web Security appliance to have stricter access requirements for administrators logging into the appliance.

Command	Description
adminaccessconfig > banner	<p>Configures the appliance to display any text you specify when an administrator tries to log in. The custom banner text appears when an administrator tries to access the appliance through all interfaces, such as the web interface or via FTP.</p> <p>You can load the custom text by either pasting it into the CLI prompt or by copying it from a file located on the Web Security appliance. To upload the text from a file, you must first transfer the file to the configuration directory on the appliance using FTP.</p>
adminaccessconfig > ipaccess	<p>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.</p> <p>When restrict access to an allow list, you can specify IP addresses, subnets, or CIDR addresses.</p> <p>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.</p>
adminaccessconfig > strictssl	<p>Configures the appliance so administrators log into the web interface on port 8443 using stronger SSL ciphers (greater than 56 bit encryption).</p> <p>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.</p>

## Resetting the Administrator Passphrase

Any administrator-level user can change the passphrase for the “admin” user.

### 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.

---

**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.

---

# Managing Alerts

Alerts are email notifications containing information about events occurring on the Cisco Web Security Appliance appliance. These events can be of varying levels of importance (or severity) from minor (Informational) to major (Critical) and pertain generally to a specific component or feature on the appliance.



**Note** To receive alerts and email notifications, you must configure the SMTP relay host that the appliance uses to send the email messages.

## Alert Classifications and Severities

The information contained in an alert is determined by an alert classification and a severity. You can specify which alert classifications, at which severity, are sent to any alert recipient.

### Alert Classifications

AsyncOS sends the following types of alert:

- System
- Hardware
- Updater
- Web Proxy
- Anti-Malware
- L4 Traffic Monitor

### Alert Severities

Alerts can be sent for the following severities:

- **Critical:** Requires immediate attention.
- **Warning:** Problem or error requiring further monitoring and potentially immediate attention.
- **Information:** Information generated in the routine functioning of this device.

# Managing Alert Recipients



**Note** If you enabled AutoSupport during System Setup, the email address you specified will receive alerts for all severities and classes by default. You can change this configuration at any time.

## Adding and Editing Alert Recipients

- 
- Step 1** Choose **System Administration > Alerts**.
  - Step 2** Click on a recipient in the Alert Recipients list to edit it, or click **Add Recipient** to add a new recipient.
  - Step 3** Add or edit the recipient's email address. You can enter multiple addresses, separated by commas.

- 
- Step 4** Select which alert severities to receive for each alert type.
- Step 5** Submit and commit your changes.
- 

## Deleting Alert Recipients

- 
- Step 1** Choose **System Administration > Alerts**.
- Step 2** Click the trash can icon corresponding to the alert recipient in the Alert Recipient listing and confirm.
- Step 3** Commit your changes.
- 

## Configuring Alert Settings

Alert settings are global settings, meaning that they affect how all of the alerts behave.

- 
- Step 1** Choose **System Administration > Alerts**.
- Step 2** Click **Edit Settings**.
- Step 3** Configure the alert settings as required.

Option	Description
From Address to Use When Sending Alerts	The RFC 2822 compliant “Header From:” address to use when sending alerts. An option is provided to automatically generate an address based on the system hostname (“alert@<hostname>”)

## ■ Managing Alerts

Option	Description
Wait Before Sending a Duplicate Alert	<p>Specifies the time interval for duplicate alerts. There are two settings:</p> <p><b>Initial Number of Seconds to Wait Before Sending a Duplicate Alert.</b> 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.</p> <p><b>Maximum Number of Seconds to Wait Before Sending a Duplicate Alert.</b> 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</p>
Cisco AutoSupport	<p>Specifies whether or not to send Cisco the following support information:</p> <ul style="list-style-type: none"> <li>• a copy of all alert messages generated by the system</li> <li>• weekly reports noting the uptime of the system, the output of the <code>status</code> command, and the AsyncOS version used.</li> </ul> <p>Also specifies whether or not to send internal alert recipients a copy of every message sent to Cisco. This applies only to recipients that are set to receive System alerts at Information severity level.</p>

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

---

## Alert Listing

The following sections list alerts by classification. The table in each section includes the alert name (internally used descriptor), actual text of the alert, description, severity (critical, information, or warning) and the parameters (if any) included in the text of the message.

## Feature Key Alerts

The following table contains a list of the various feature key alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
A “\$feature” key was downloaded from the key server and placed into the pending area. EULA acceptance required.	Information.	<b>\$feature:</b> Name of the feature.

Message	Alert Severity	Parameters
Your “\$feature” evaluation key has expired. Please contact your authorized sales representative.	Warning.	<b>\$feature:</b> Name of the feature.
Your “\$feature” evaluation key will expire in under \$days day(s). Please contact your authorized sales representative.	Warning.	<b>\$feature:</b> Name of the feature. <b>\$days:</b> The number of days that will pass before the feature key will expire.

## Hardware Alerts

The following table contains a list of the various hardware alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
A RAID-event has occurred:	Warning	<b>\$error:</b> Text of the RAID error.
\$error		

## Logging Alerts

The following table contains a list of the various logging alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
\$error.	Information.	<b>\$error:</b> The traceback string of the error.
Log Error: Subscription \$name: Log partition is full.	Critical.	<b>\$name:</b> Log subscription name.
Log Error: Push error for subscription \$name: Failed to connect to \$ip: \$reason.	Critical.	<b>\$name:</b> Log subscription name. <b>\$ip:</b> IP address of the remote host. <b>\$reason:</b> Text describing the connect error
Log Error: Push error for subscription \$name: An FTP command failed to \$ip: \$reason.	Critical.	<b>\$name:</b> Log subscription name. <b>\$ip:</b> IP address of the remote host. <b>\$reason:</b> Text describing what went wrong.
Log Error: Push error for subscription \$name: SCP failed to transfer to \$ip:\$port: \$reason',	Critical.	<b>\$name:</b> Log subscription name. <b>\$ip:</b> IP address of the remote host. <b>\$port:</b> Port number on the remote host. <b>\$reason:</b> Text describing what went wrong.
Log Error: 'Subscription \$name: Failed to connect to \$hostname (\$ip): \$error.	Critical.	<b>\$name:</b> Log subscription name. <b>\$hostname:</b> Hostname of the syslog server. <b>\$ip:</b> IP address of the syslog server. <b>\$error:</b> Text of the error message.

## ■ Managing Alerts

Message	Alert Severity	Parameters
Log Error: Subscription \$name: Network error while sending log data to syslog server \$hostname (\$ip): \$error	Critical.	<b>\$name:</b> Log subscription name. <b>\$hostname:</b> Hostname of the syslog server. <b>\$ip:</b> IP address of the syslog server. <b>\$error:</b> Text of the error message.
Subscription \$name: Timed out after \$timeout seconds sending data to syslog server \$hostname (\$ip).	Critical.	<b>\$name:</b> Log subscription name. <b>\$timeout:</b> Timeout in seconds. <b>\$hostname:</b> Hostname of the syslog server. <b>\$ip:</b> IP address of the syslog server.
Subscription \$name: Syslog server \$hostname (\$ip) is not accepting data fast enough.	Critical.	<b>\$name:</b> Log subscription name. <b>\$hostname:</b> Hostname of the syslog server. <b>\$ip:</b> IP address of the syslog server.
Subscription \$name: Oldest log file(s) were removed because log files reached the maximum number of \$max_num_files. Files removed include: \$files_removed.	Information.	<b>\$name:</b> Log subscription name. <b>\$max_num_files:</b> Maximum number of files allowed per log subscription. <b>\$files_removed:</b> 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'.	Critical.	<b>\$report_title:</b> Title of the report.
This subscription should be examined and deleted if its configuration details are no longer valid.		
A failure occurred while emailing periodic report '\$report_title'.	Critical.	<b>\$report_title:</b> Title of the report.
This subscription has been removed from the scheduler.		

Message	Alert Severity	Parameters
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).	Warning.	<b>\$threshold:</b> Threshold value.
Once disk usage drops below \$threshold percent, full processing of reporting data will be restarted automatically.		
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.	<b>\$report_title:</b> Title of the report. <b>\$file_name:</b> Name of the file.
Counter group "\$counter_group" does not exist.	Critical.	<b>\$counter_group:</b> 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.	<b>\$report_title:</b> Title of the report. <b>\$file_name:</b> 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.  \$error_text	Critical.	<b>\$report_title:</b> Title of the report. <b>\$file_name:</b> Name of the file. <b>\$error_text:</b> 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).	Warning.	<b>\$threshold:</b> Threshold value.
Once disk usage drops below \$threshold percent, full processing of reporting data will be restarted automatically.		
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.  The error message is:  \$err_msg	Critical.	<b>\$err_msg:</b> Error message text.

## System Alerts

The following table contains a list of the various system alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
Startup script \$name exited with error: \$message	Critical.	<b>\$name:</b> Name of the script. <b>\$message:</b> Error message text.
System halt failed: \$exit_status: \$output',	Critical.	<b>\$exit_status:</b> Exit code of the command. <b>\$output:</b> Output from the command.
System reboot failed: \$exit_status: \$output	Critical.	<b>\$exit_status:</b> Exit code of the command. <b>\$output:</b> Output from the command.
Process \$name listed \$dependency as a dependency, but it does not exist.	Critical.	<b>\$name:</b> Name of the process. <b>\$dependency:</b> Name of the dependency that was listed.
Process \$name listed \$dependency as a dependency, but \$dependency is not a wait_init process.	Critical.	<b>\$name:</b> Name of the process. <b>\$dependency:</b> Name of the dependency that was listed.
Process \$name listed itself as a dependency.	Critical.	<b>\$name:</b> Name of the process.
Process \$name listed \$dependency as a dependency multiple times.	Critical.	<b>\$name:</b> Name of the process. <b>\$dependency:</b> Name of the dependency that was listed.
Dependency cycle detected: \$cycle.	Critical.	<b>\$cycle:</b> The list of process names involved in the cycle.
An error occurred while attempting to share statistical data through the Network Participation feature. Please forward this tracking information to your support provider:  Error: \$error.	Warning.	<b>\$error:</b> The error message associated with the exception.
There is an error with “\$name”.	Critical.	<b>\$name:</b> Name of the process that generated a core file.
An application fault occurred: “\$error”	Critical.	<b>\$error:</b> Text of the error, typically a traceback.
Tech support: Service tunnel has been enabled, port \$port	Information.	<b>\$port:</b> Port number used for the service tunnel.

Message	Alert Severity	Parameters
Tech support: Service tunnel has been disabled.	Information.	Not applicable.
<ul style="list-style-type: none"> <li>The host at \$ip has been added to the blacklist because of an SSH DOS attack.</li> <li>The host at \$ip has been permanently added to the ssh whitelist.</li> <li>The host at \$ip has been removed from the blacklist</li> </ul>	Warning.	<p><b>\$ip</b> - IP address from which a login attempt occurred.</p> <p><b>Description:</b> IP addresses that try to connect to the appliance over SSH but do not provide valid credentials are added to the SSH blacklist if more than 10 failed attempts occur within two minutes.</p> <p>When a user logs in successfully from the same IP address, that IP address is added to the whitelist.</p> <p>Addresses on the whitelist are allowed access even if they are also on the blacklist.</p> <p>Entries are automatically removed from the blacklist after about a day.</p>

## Updater Alerts

The following table contains a list of the various updater alerts that can be generated by AsyncOS, including a description of the alert and the alert severity:

Message	Alert Severity	Parameters
The \$app application tried and failed \$attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage.	Warning.	<p><b>\$app:</b> Web Security appliance security service name.</p> <p><b>\$attempts:</b> Number of attempts tried.</p>
The updater has been unable to communicate with the update server for at least \$threshold.	Warning.	<b>\$threshold:</b> Threshold value time.
Unknown error occurred: \$traceback.	Critical.	<b>\$traceback:</b> Traceback information.

## Anti-Malware Alerts

For information about alerts related to Advanced Malware Protection, see [Ensuring That You Receive Alerts About Advanced Malware Protection Issues, page 14-10](#).

# System Date and Time Management

- [Setting the Time Zone, page 12-22](#)
- [Synchronizing the System Clock with an NTP Server, page 12-22](#)

## Setting the Time Zone

- 
- Step 1** Choose **System Administration > Time Zone**.
  - Step 2** Click **Edit Settings**.
  - Step 3** Select your region, country, and time zone or select the GMT offset.
  - Step 4** Submit and commit the changes.
- 

## Synchronizing the System Clock with an NTP Server

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.

- 
- 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, page B-6](#).

- 
- 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.
  - **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/apps/ciphers.html> for additional information, and cipher lists.

The default cipher for AsyncOS versions 9.0 and earlier is `DEFAULT:+kEDH`. For AsyncOS versions 9.1 and later, it the default cipher is

`ECDH: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 both cases, this may change based on your ECDHE cipher selections.



**Note** However, regardless of version, the default cipher does not change when you upgrade to a newer AsyncOS version. For example, when you upgrade from an earlier version to AsyncOS 9.1, the default cipher is `DEFAULT:+kEDH`. In other words, following an upgrade, you must update the current cipher suite yourself; Cisco recommends updating to

`ECDH: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`.

- 
- **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, page 16-9](#) 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, page 12-27](#) 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.

## Related Topics

- [About Certificates and Keys, page 12-24](#)
- [Certificate Updates, page 12-25](#)
- [Managing Trusted Root Certificates, page 12-24](#)
- [Viewing Blocked Certificates, page 12-25](#)

## 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, page 12-25](#)
- [Certificate Signing Requests, page 12-26](#)
- [Intermediate Certificates, page 12-27](#)

## 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 master 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:

- 
- 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:
- Click the name of the certificate in the Cisco Trusted Root Certificate List to expand that entry.
  - Click **Download Certificate**.
- 

## Certificate Updates

The Updates section lists version and last-updated information for the Cisco trusted-root-certificate and blacklist bundles on the appliance. These bundles are updated periodically.

---

- Step 1** 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:

---

- Step 1** 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. 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.
- 

- 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

**Step 1** Select **Use Generated Certificate and Key**.

**Step 2** Click **Generate New Certificate and Key**.

- 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.

- 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, page 12-26](#) for more information about this process.

- 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.
- 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, page 12-24](#) 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](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.

# 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.

In Hybrid mode, upgrades are downloaded automatically whenever available, and then installed during a specified time window. To change the current time window:

---

**Step 1** Choose **System Administration > Upgrade and Update Settings**.

**Step 2** Click **Edit Upgrade Timing**.

**Step 3** Define the Upgrade Time Window by choosing the **Day of Week** and the hour and minute of the **Time** at which the upgrade installation can start.

You are defining the start of a two-hour window during which upgrades/updates installation may begin. Since the appliance will reboot when installation is completed, specify the least-disruptive time possible.

**Step 4** To reschedule the next upgrade installation, check **Set Exception for Next Target Upgrade** then select the **Exception Date** and choose the hour and minute of the exception start **Time**.

This is a one-time exception that overrides the default day/time once, meaning you can install a pending upgrade before the default day/time, or you can set a “blackout window” during which the default day/time is ignored and the upgrade installed on the later day/time.

**Step 5** Click **Submit**.

---

# 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 appliances.
- `ASYNCO-S-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.

## 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, page C-2](#)

## SNMP Traps

SNMP provides the ability to send traps, or notifications, to advise an administration application when one or more conditions have been met. Traps are network packets that contain data relating to a component of the system sending the trap. Traps are generated when a condition has been met on the SNMP agent (in this case, the Cisco Web Security Appliance appliance). After the condition has been met, the SNMP agent then forms an SNMP packet and sends it 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, page 12-29](#)

## 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 connectivityFailure 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
```

**■ Monitoring System Health and Status Using SNMP**

```

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>
```

**■ Monitoring System Health and Status Using SNMP**



APPENDIX

A

## Troubleshooting

---

- General Troubleshooting Best Practices
- Hybrid Web Security Issues
- Blocked Object Problems
- Browser Problems
- DNS Problems
- Failover Problems
- Feature Keys Expired
- FTP Problems
- Hardware Issues
- HTTPS/Decryption/Certificate Problems
- Logging Problems
- Policy Problems
- Reboot Issues
- Site Access Problems
- Upstream Proxy Problems
- Virtual Appliances
- WCCP Problems
- Packet Capture
- Working With Support

## 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, page 11-30](#).

For configuration instructions, see [Customizing Access Logs, page 11-26](#) and [Adding and Editing Log Subscriptions, page 11-7](#).

# Hybrid Web Security Issues

- Registration (including Enrollment)
- Policy Download
- Policy Conversion
- Hybrid Upgrade

## Registration (including Enrollment)

- Connection errors between API gateway and Enrollment over Secure Transport (EST) server – Set logs to Trace level, capture logs, contact Support.
- Connection failure due to API gateway and EST server root certificates not present on WSA – Set logs to Trace level, capture logs, contact Support.
- Invalid authentication key – Try a new key; if that fails, contact Support.

## Policy Download

- Connection errors with API gateway – Contact Support.

## Policy Conversion

- AVC mismatch – Force an update on the WSA using the CLI `updatenow` command; if that fails, contact Support.
- Dynamic updates not received for various modules like AVC, Sophos, etc. – Force an update on the WSA using the CLI `updatenow` command; if that fails, contact Support.
- Conversion taking too long (more than 20 minutes) and timing-out – Contact Support.

## Hybrid Upgrade

- Connection errors – Contact Support.
- Upgrade server certificate validation failure – Check connectivity with upgrade server; if that fails, contact Support.
- Upgrade image download fails – Check connectivity with the upgrade server; if that fails, contact Support.
- Upgrade itself fails – Contact Support.
- Upgrade timing window configuration error – Check the time zone configured on the WSA with the Software Setup Wizard.

## Browser Problems

- WPAD Not Working With Firefox

## 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](https://bugzilla.mozilla.org/show_bug.cgi?id=356831).

To use Firefox (or any other browser that does not support DHCP) with WPAD when the PAC file is hosted on the Web Security appliance, configure the appliance to serve the PAC file through port 80.

- 
- Step 1** Choose **Security Services > Web Proxy** and delete port 80 from the **HTTP Ports to Proxy** field.
  - Step 2** Use port 80 as the PAC Server Port when you upload the file to the appliance.
  - Step 3** If any browsers are manually configured to point to the web proxy on port 80, reconfigure those browsers to point to another port in the HTTP Ports to Proxy field.
  - Step 4** Change any references to port 80 in PAC files.
- 

## DNS Problems

- [Alert: Failed to Bootstrap the DNS Cache](#)

### Alert: Failed to Bootstrap the DNS Cache

If an alert with the message “Failed to bootstrap the DNS cache” is generated when an appliance is rebooted, it means that the system was unable to contact its primary DNS servers. This can happen at boot time if the DNS subsystem comes online before network connectivity is established. If this message appears at other times, it could indicate network issues or that the DNS configuration is not pointing to a valid server.

## Feature Keys Expired

If the feature key for the feature you are trying to access (via the web interface) has expired, please contact your Cisco representative or support organization.

## Failover Problems

- [Failover Misconfiguration](#)
- [Failover Issues on Virtual Appliances](#)

### Failover Misconfiguration

Misconfiguration of failover groups might result in multiple master 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: MASTER
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.

## FTP Problems

- [URL Categories Do Not Block Some FTP Sites](#)
- [Large FTP Transfers Disconnect](#)
- [Zero Byte File Appears On FTP Servers After File Upload](#)
- [Chrome Browser Not Detected As User Agent in FTP-over-HTTP Requests, page A-5](#)
- Also see:
  - [Unable to Route FTP Requests Via an Upstream Proxy](#)
  - [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication](#)

## URL Categories Do Not Block Some FTP Sites

When a native FTP request is transparently redirected to the FTP Proxy, it contains no hostname information for the FTP server, only its IP address. Because of this, some predefined URL categories and Web Reputation Filters that have only hostname information will not match native FTP requests, even if the requests are destined for those servers. If you wish to block access to these sites, you must create custom URL categories for them using their IP addresses.

## Large FTP Transfers Disconnect

If the connection between the FTP Proxy and the FTP server is slow, uploading a large file may take a long time, particularly when Cisco Data Security Filters are enabled. This can cause the FTP client to time out before the FTP Proxy uploads the entire file and you may get a failed transaction notice. The transaction does not fail, however, but continues in the background and will be completed by the FTP Proxy.

You can 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.

## Hardware Issues

- [Cycling Appliance Power, page A-5](#)
- [Appliance Health and Status Indicators, page A-5](#)
- [Alert: Battery Relearn Timed Out \(RAID Event\) on 380 or 680 Hardware, page A-5](#)

## Cycling Appliance Power

**Important!** If you need to cycle power to your x80 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 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.

- [Accessing HTTPS Sites Using Routing Policies with URL Category Criteria](#)
- [HTTPS Request Failures](#)
- [Bypassing Decryption for Particular Websites](#)
- [Conditions and Restrictions for Exceptions to Blocking for Embedded and Referred Content](#)
- [Alert: Problem with Security Certificate](#)
- Also see:
  - [Logging HTTPS Transactions](#)
  - [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication](#)

## Accessing HTTPS Sites Using Routing Policies with URL Category Criteria

For transparently redirected HTTPS requests, the Web Proxy must contact the destination server to determine the server name and therefore the URL category in which it belongs. Due to this, when the Web Proxy evaluates Routing Policy Group membership, it cannot yet know the URL category of an HTTPS request because it has not yet contacted the destination server. If the Web Proxy does not know the URL category, it cannot match the transparent HTTPS request to a Routing Policy that uses a URL category as membership criteria.

As a result, transparently redirected HTTPS transactions only match Routing Policies that do not define Routing Policy Group membership criteria by URL category. If all user-defined Routing Policies define their membership by URL category, transparent HTTPS transactions match the Default Routing Policy Group.

## HTTPS Request Failures

- [HTTPS with IP-based Surrogates and Transparent Requests](#)
- [Different Client “Hello” Behavior for Custom and Default Categories](#)

## HTTPS with IP-based Surrogates and Transparent Requests

If the HTTPS request comes from a client that does not have authentication information available from an earlier HTTP request, AsyncOS either fails the HTTPS request or decrypts the HTTPS request in order to authenticate the user, depending on how you configure the HTTPS Proxy. Use the HTTPS Transparent Request setting on the Security Services > HTTPS Proxy page to define this behavior. Refer to the Enabling HTTPS Proxy section in Decryption Policies chapter.

## 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.

- 
- 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:

- 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.

## Logging Problems

- [Custom URL Categories Not Appearing in Access Log Entries](#)
- [Logging HTTPS Transactions](#)
- [Alert: Unable to Maintain the Rate of Data Being Generated](#)
- [Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs](#)

## Custom URL Categories Not Appearing in Access Log Entries

When a web access policy group has a custom URL category set to Monitor and some other component, such as the Web Reputation Filters or the DVS engine, makes the final decision to allow or block a request for a URL in the custom URL category, then the access log entry for the request shows the predefined URL category instead of the custom URL category.

## Logging HTTPS Transactions

HTTPS transactions in the access logs appear similar to HTTP transactions, but with slightly different characteristics. What gets logged depends on whether the transaction was explicitly sent or transparently redirected to the HTTPS Proxy:

- **TUNNEL.** This gets written to the access log when the HTTPS request was transparently redirected to the HTTPS Proxy.
- **CONNECT.** This gets written to the access log when the HTTPS request was explicitly sent to the HTTPS Proxy.

When HTTPS traffic is decrypted, the access logs contain two entries for a transaction:

- TUNNEL or CONNECT depending on the type of request processed.
- The HTTP Method and the decrypted URL. For example, "GET https://ftp.example.com".

The full URL is only visible when the HTTPS Proxy decrypts the traffic.

## Alert: Unable to Maintain the Rate of Data Being Generated

AsyncOS for Web sends a critical email message to the configured alert recipients when the internal logging process drops web transaction events due to a full buffer.

By default, when the Web Proxy experiences a very high load, the internal logging process buffers events to record them later when the Web Proxy load decreases. When the logging buffer fills completely, the Web Proxy continues to process traffic, but the logging process does not record some events in the access logs or in the Web Tracking report. This might occur during a spike in web traffic.

However, a full logging buffer might also occur when the appliance is over capacity for a sustained period of time. AsyncOS for Web continues to send the critical email messages every few minutes until the logging process is no longer dropping data.

The critical message contains the following text:

Reporting Client: The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.

If AsyncOS for Web sends this critical message continuously or frequently, the appliance might be over capacity. Contact Cisco Customer Support to verify whether or not you need additional Web Security appliance capacity.

## Problem Using Third-Party Log-Analyzer Tool with W3C Access Logs

If you want to use a third party log analyzer tool to read and parse the W3C access logs, you might need to include the “timestamp” field. The timestamp W3C field displays time since the UNIX epoch, and most log analyzers only understand time in this format.

## Policy Problems

- [Blocked Object Problems](#)
- [Identification Profile Disappeared from Policy](#)
- [Policy Match Failures](#)
- Also see: [Accessing HTTPS Sites Using Routing Policies with URL Category Criteria](#)

## Blocked Object Problems

- [Some Microsoft Office Files Not Blocked](#)
- [Blocking DOS Executable Object Types Blocks Updates for Windows OneCare](#)

### Some Microsoft Office Files Not Blocked

When you block Microsoft Office files in the Block Object Type section, it is possible that some Microsoft Office files will not be blocked.

If you need to block all Microsoft Office files, add `application/x-ole` in the Block Custom MIME Types field. However, blocking this custom MIME type also blocks all Microsoft Compound Object format types, such as Visio files and some third-party applications.

## Blocking DOS Executable Object Types Blocks Updates for Windows OneCare

When you configure the Web Security appliance to block DOS executable object types, the appliance also blocks updates for Windows OneCare.

## 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](#)
- [HTTPS and FTP over HTTP Requests Match only Access Policies that Do Not Require Authentication](#)
- [User Matches Global Policy for HTTPS and FTP over HTTP Requests](#)
- [User Assigned Incorrect Access Policy](#)

## Policy is Never Applied

If multiple 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.

---

**Step 1** Use the advancedproxyconfig > authentication CLI command.

**Step 2** Enter the surrogate timeout for machine credentials.

---

## Reboot Issues

- Virtual Appliance Running on KVM Hangs on Reboot
- Hardware Appliances: Remotely Resetting Appliance Power

## 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>.

---

**Step 1** Check the following:

```
cat /sys/module/kvm_intel/parameters/enable_apicv
```

**Site Access Problems**

**Step 2** If the above value is set to Y:

- a. Stop your virtual appliances and reinstall the KVM kernel module:

```
rmmmod kvm_intel
modprobe kvm_intel enable_apicv=N
```

- b. Restart your virtual appliance.
- 

## Hardware Appliances: Remotely Resetting Appliance Power

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, page 12-5](#).
- 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, page 12-5](#).
- Only the following IPMI commands are supported: status, on, off, cycle, reset, diag, soft. Issuing unsupported commands will produce an “insufficient privileges” error.

### 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.
- 

**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
```

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](#)
- [Cannot Access Sites With POST Requests](#)
- Also see: [Bypassing Decryption for Particular Websites](#)

## Cannot Access URLs that Do Not Support Authentication

This is a partial list of applications cannot be used when the Web Security appliance is deployed in transparent mode because they do not support authentication.

- Mozilla Thunderbird
- Adobe Acrobat Updates
- HttpBridge
- Subversion, by CollabNet
- Microsoft Windows Update
- Microsoft Visual Studio

Workaround: Create a class of user for the URL that does not require authentication.

### Related Topics

- [Bypassing Authentication, page 5-31](#)

## 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, page 5-31](#).

# Upstream Proxy Problems

- Upstream Proxy Does Not Receive Basic Credentials
- Client Requests Fail Upstream Proxy

## Upstream Proxy Does Not Receive Basic Credentials

If both the appliance and the upstream proxy use authentication with NTLMSSP, depending on the configurations, the appliance and upstream proxy might engage in an infinite loop of requesting authentication credentials. For example, if the upstream proxy requires Basic authentication, but the appliance requires NTLMSSP authentication, then the appliance can never successfully pass Basic credentials to the upstream proxy. This is due to limitations in authentication protocols.

## Client Requests Fail Upstream Proxy

Configuration:

- Web Security appliance and upstream proxy server use Basic authentication.
- Credential Encryption is enabled on the downstream Web Security appliance.

Client requests fail on the upstream proxy because the Web Proxy receives an “Authorization” HTTP header from clients, but the upstream proxy server requires a “Proxy-Authorization” HTTP header.

## Unable to Route FTP Requests Via an Upstream Proxy

If your network contains an upstream proxy that does not support FTP connections, then you must create a Routing Policy that applies to all Identities and to just FTP requests. Configure that Routing Policy to directly connect to FTP servers or to connect to a proxy group whose proxies all support FTP connections.

# Virtual Appliances

- Do Not Use Force Reset, Power Off, or Reset Options During AsyncOS Startup
- Network Connectivity on KVM Deployments Works Initially, Then Fails
- Slow Performance, Watchdog Issues, and High CPU Usage on KVM Deployments
- General Troubleshooting for Virtual Appliances Running on Linux Hosts

## 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](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](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

### 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
- Managing Packet Capture Files

The appliance provides the ability to capture and display TCP/IP and other packets being transmitted or received over the network to which the appliance is attached.



Note

The packet capture feature is similar to the Unix tcpdump command.

## Starting a Packet Capture

**Step 1** Choose Support and Help > Packet Capture.

**Step 2** (Optional) Click **Edit Settings** to change the packet capture settings.

Option	Description
Capture File Size Limit	Specifies the maximum size that the capture file can reach. Once the limit is reached, the data will be discarded and a new file started, unless the Capture Duration setting is 'Run Capture Until File Size Limit Reached.'
Capture Duration	Options for if and when the capture automatically stops. Choose from: <ul style="list-style-type: none"> <li><b>Run Capture Until File Size Limit Reached.</b> The capture runs until the file limit set above is reached.</li> <li><b>Run Capture Until Time Elapsed Reaches.</b> The capture runs for a specified duration. If you enter the amount of time without specifying the units, AsyncOS uses seconds by default.</li> <li><b>Run Capture Indefinitely.</b> The packet capture runs until you manually stop it.</li> </ul> <b>Note</b> 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: <ul style="list-style-type: none"> <li><b>No Filters.</b> All packets will be captured.</li> <li><b>Predefined Filters.</b> The predefined filters provide filtering by port and/or IP addresses. If left blank, all traffic will be captured.</li> <li><b>Custom Filter.</b> Use this option if you already know the exact syntax of the packet capture options that you need. Use standard tcpdump syntax.</li> </ul>

(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](#)

## 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.

---

**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, page A-17](#)
- [Opening a Technical Support Request, page A-17](#)
- [Getting Support for Virtual Appliances, page A-18](#)
- [Enabling Remote Access to the Appliance, page A-18](#)

## Gathering Information for Efficient Service

Before contacting Support:

- Enable custom logging fields as described in [General Troubleshooting Best Practices, page A-1](#).
- Consider doing a packet capture. See [Packet Capture, page A-15](#).

## Opening a Technical Support Request

You can use the appliance to send a non-urgent request for assistance to Cisco Customer Support. When the appliance sends the request, it also sends the configuration of the appliance. The appliance must be able to send mail to the Internet to send a support request.

**Note**

---

If you have an urgent issue, please call a Cisco Worldwide Support Center.

---

### Before You Begin

- Verify that your Cisco.com user ID is associated with your service agreement contract for this appliance. To view a list of service contracts that are currently associated with your Cisco.com profile, visit the Cisco.com Profile Manager at <https://sso.cisco.com/autho/forms/CDClogin.html>. If you do not have a Cisco.com user ID, register to get one.

---

**Step 1** Choose **Support And Help > Contact Technical Support**.

- Step 2** (Optional) Choose additional recipients for the request. By default, the support request and configuration file is sent to Cisco Customer Support.
- Step 3** Enter your contact information.
- Step 4** Enter the issue details.
- If you have a customer support ticket already for this issue, enter it.
- Step 5** Click **Send**. A trouble ticket is created with Cisco.
- 

## 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: <ul style="list-style-type: none"> <li>• Web Usage Controls</li> <li>• Web Reputation</li> </ul>
Web Security Premium	WSA-WSP-LIC=	Includes: <ul style="list-style-type: none"> <li>• Web Usage Controls</li> <li>• Web Reputation</li> <li>• Sophos and Webroot Anti-Malware signatures</li> </ul>
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.

- 
- 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.  The string will appear near the top of the page after you click Submit.  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.  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.  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.  The Remote Access account will remain active until specifically deactivated.

**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.





## Command Line Interface

---

- [Overview of the Command Line Interface, page 27-1](#)
- [Accessing the Command Line Interface, page 27-1](#)
- [General Purpose CLI Commands, page 27-4](#)
- [Web Security Appliance CLI Commands, page 27-6](#)

## Overview of the Command Line Interface

The AsyncOS Command Line Interface (CLI) allows you to configure and monitor the Web Security appliance. The Command Line Interface is accessible using SSH on IP interfaces that have been configured with these services enabled, or using terminal emulation software on the serial port. By default, SSH is configured on the Management port.

The commands are invoked by entering the command name with or without any arguments. If you enter a command without arguments, the command prompts you for the required information.

## Accessing the Command Line Interface

You can 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, page 12-6](#) 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, typing Enter or Return at an empty prompt returns you to the main command.

## Escaping Subcommands

You can use the Ctrl+C keyboard shortcut at any time within a subcommand to immediately exit return to the top level of the CLI.

## Command History

The CLI keeps a history of all commands entered during a session. Use the Up and Down arrow keys on your keyboard, or the Ctrl+P and Ctrl+N key combinations to scroll through a running list of the recently-used commands.

## Completing Commands

The AsyncOS CLI supports command completion. You can enter the first few letters of some commands followed by the Tab key and the CLI completes the string. If the letters you entered are not unique among commands, the CLI “narrows” the set. For example:

```
example.com> set (press the Tab key)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth (pressing the Tab again completes the entry with 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, page 27-6.](#)

# Web Security Appliance CLI Commands

The Web Security Appliance CLI supports a set of proxy and UNIX commands to access, upgrade, and administer the system.



**Note** Not all CLI commands are applicable/available in all operating modes (Standard Cloud Web Security Connector, and Hybrid Web Security).

Command	Description
advancedproxyconfig	<p>Configure advanced Web Proxy configurations; subcommands are:</p> <p><b>AUTHENTICATION</b> – Authentication configuration options:</p> <ul style="list-style-type: none"> <li>• When would you like to forward authorization request headers to a parent proxy</li> <li>• Enter the Proxy Authorization Realm to be displayed in the end user authentication dialog</li> <li>• Would you like to log the username that appears in the request URI</li> <li>• 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)</li> <li>• Would you like to use advanced Active Directory connectivity checks</li> <li>• Would you like to allow case insensitive username matching in policies</li> <li>• Would you like to allow wild card matching with the character * for LDAP group names</li> <li>• Enter the charset used by the clients for basic authentication [ISO-8859-1/UTF-8]</li> <li>• Would you like to enable referrals for LDAP</li> <li>• Would you like to enable secure authentication</li> <li>• Enter the hostname to redirect clients for authentication</li> <li>• Enter the surrogate timeout for user credentials</li> <li>• Enter the surrogate timeout for machine credentials</li> <li>• Enter the surrogate timeout in the case traffic permitted due to authentication service unavailability</li> <li>• Enter re-auth on request denied option [disabled / embedlinkinblockpage]</li> <li>• Would you like to send Negotiate header along with NTLM header for NTLMSSP authentication</li> <li>• Configure username and IP address masking in logs and reports</li> </ul>

---

advancedproxyconfig (cont.)	<p><b>CACHING</b> – Proxy Caching mode; choose one:</p> <ul style="list-style-type: none"> <li>• Safe Mode</li> <li>• Optimized Mode</li> <li>• Aggressive Mode</li> <li>• Customized Mode</li> </ul> <p>See also <a href="#">Choosing The Web Proxy Cache Mode, page 4-6</a>.</p> <p><b>DNS</b> – DNS configuration options:</p> <ul style="list-style-type: none"> <li>• Enter the URL format for the HTTP 307 redirection on DNS lookup failure</li> <li>• Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure</li> <li>• Would you like proxy not to automatically failover to DNS results when upstream proxy (peer) is unresponsive</li> <li>• Find web server by:           <ul style="list-style-type: none"> <li>0 = Always use DNS answers in order</li> <li>1 = Use client-supplied address then DNS</li> <li>2 = Limited DNS usage</li> <li>3 = Very limited DNS usage</li> </ul> </li> </ul> <p>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.</p> <p><b>EUN</b> – End-user notification parameters:</p> <ul style="list-style-type: none"> <li>• Choose:           <ol style="list-style-type: none"> <li>1. Refresh EUN pages</li> <li>2. Use Custom EUN pages</li> <li>3. Use Standard EUN pages</li> </ol> </li> <li>• Would you like to turn on presentation of the User Acknowledgement page?</li> </ul> <p>See also <a href="#">Web Proxy Usage Agreement, page 4-10</a> and <a href="#">End-User Notifications Overview, page 9-1</a>.</p> <p><b>NATIVEFTP</b> – Native FTP configuration:</p> <ul style="list-style-type: none"> <li>• Would you like to enable FTP proxy</li> <li>• Enter the ports that FTP proxy listens on</li> <li>• Enter the range of port numbers for the proxy to listen on for passive FTP connections</li> <li>• Enter the range of port numbers for the proxy to listen on for active FTP connections</li> <li>• Enter the authentication format:           <ol style="list-style-type: none"> <li>1. Check Point</li> <li>2. No Proxy Authentication</li> <li>3. Raptor</li> </ol> </li> <li>• Would you like to enable caching</li> <li>• Would you like to enable server IP spoofing</li> <li>• Would you like to pass FTP server welcome message to the clients</li> <li>• Enter the max path size for the ftp server directory</li> </ul>
--------------------------------	---

---

---

advancedproxyconfig (continued)	<p><b>FTP OVER HTTP</b> – FTP Over HTTP options:</p> <ul style="list-style-type: none"> <li>• Enter the login name to be used for anonymous FTP access</li> <li>• Enter the password to be used for anonymous FTP access</li> </ul> <p><b>HTTPS</b> – HTTPS-related options:</p> <ul style="list-style-type: none"> <li>• HTTPS URI Logging Style - fulluri or stripquery</li> <li>• Would you like to decrypt unauthenticated transparent HTTPS requests for authentication purpose</li> <li>• Would you like to decrypt HTTPS requests for End User Notification purpose</li> <li>• Action to be taken when HTTPS servers ask for client certificate during handshake:           <ol style="list-style-type: none"> <li>1. Pass through the transaction</li> <li>2. Reply with certificate unavailable</li> </ol> </li> <li>• Do you want to enable server name indication (SNI) extension?</li> <li>• Do you want to enable automatic discovery and download of missing Intermediate Certificates?</li> <li>• Do you want to enable session resumption?</li> </ul> <p>See also <a href="#">Overview of Create Decryption Policies to Control HTTPS Traffic, page 7-1</a>.</p> <p><b>SCANNING</b> – Scanning options:</p> <ul style="list-style-type: none"> <li>• Would you like the proxy to do malware scanning all content regardless of content type</li> <li>• Enter the time to wait for a response from an anti-malware scanning engine (Sophos, McAfee, or Webroot), in seconds</li> <li>• Do you want to disable Webroot body scanning</li> </ul> <p>See also <a href="#">Overview of Anti-Malware Scanning, page 8-3</a> and <a href="#">Overview of Scanning Outbound Traffic, page 12-1</a>.</p> <p><b>PROXYCONN</b> – 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.</p> <ul style="list-style-type: none"> <li>• Choose the operation you want to perform:       <ul style="list-style-type: none"> <li>NEW – Add an entry to the list of user agents</li> <li>DELETE – Remove an entry from the list</li> </ul> </li> </ul> <p><b>CUSTOMHEADERS</b> – Manage custom request headers for specific domains.</p> <ul style="list-style-type: none"> <li>• Choose the operation you want to perform:       <ul style="list-style-type: none"> <li>DELETE – Delete entries</li> <li>NEW – Add new entries</li> <li>EDIT – Edit entries</li> </ul> </li> </ul> <p>See also <a href="#">Adding Custom Headers To Web Requests, page 4-8</a>.</p>
------------------------------------	--

---

---

advancedproxyconfig  
(continued)

**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
- 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. Disable
  2. Enable for all requests
  3. Enable for transparent requests only

**Note** Spoofing is not supported in Web Hybrid mode. Please do not change any of these default values.

- Do you want to pass HTTP X-Forwarded-For headers?
- 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 URL lower case conversion for velocity regex?

See also [Using the P2 Data Interface for Web Proxy Data, page 3-22](#) and [Configuring Web Proxy Settings, page 4-3](#).

**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, page 3-22](#).

---

advancedproxyconfig (continued)	<p><b>CONTENT-ENCODING</b> – Allow and block content-encoding types.</p> <p>Currently allowed content-encoding type(s): compress, deflate, gzip</p> <p>Currently blocked content-encoding type(s): N/A</p> <p>To change the setting for a specific content-encoding type, select an option:</p> <ol style="list-style-type: none"> <li>1. compress</li> <li>2. deflate</li> <li>3. gzip</li> </ol> <p>[1]&gt;</p> <p>The encoding type "compress" is currently allowed</p> <p>Do you want to block it? [N]&gt;</p>
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.
certconfig	Configure security certificates and keys.
clear	Clears pending configuration changes since last commit.
commit	Commits pending changes to the system configuration.
createcomputerobject	Creates a computer object at the location you specify.
date	<p>Displays the current date. Example:</p> <pre>Thu Jan 10 23:13:40 2013 GMT</pre>

diagnostic	<p>Proxy- and reporting-related subcommands:</p> <p><b>NET</b> – Network Diagnostic Utility</p> <p>This command has been deprecated; use <code>packetcapture</code> to capture network traffic on the appliance.</p> <p><b>PROXY</b> – Proxy Debugging Utility</p> <p>Choose the operation you want to perform:</p> <ul style="list-style-type: none"> <li>– <b>SNAP</b> – Take a snapshot of the proxy</li> <li>– <b>OFFLINE</b> – Take the proxy off-line (via WCCP)</li> <li>– <b>RESUME</b> – Resume proxy traffic (via WCCP)</li> <li>– <b>CACHE</b> – Clear proxy cache</li> </ul> <p><b>REPORTING</b> – Reporting Utilities</p> <p>The reporting system is currently enabled.</p> <p>Choose the operation you want to perform:</p> <ul style="list-style-type: none"> <li>– <b>DELETEDB</b> – Re-initialize the reporting database</li> <li>– <b>DISABLE</b> – Disable the reporting system</li> <li>– <b>DBSTATS</b> – List DB and Export Files (Displays the list of unprocessed files and folders under <code>export_files</code> and <code>always_onbox</code> folders.)</li> <li>– <b>DELETEEXPORTDB</b> – Delete Export Files (Deletes all unprocessed files and folders under <code>export_files</code> and <code>always_onbox</code> folders.)</li> <li>– <b>DELETEJOURNAL</b> – Delete Journal Files (Deletes all <code>aclog_journal_files</code>.)</li> </ul>
dnsconfig	Configure DNS server parameters.
dnsflush	Flush DNS entries on the appliance.
etherconfig	Configure Ethernet port connections.
featurekey	Submits valid keys to activate licensed features.
featurekeyconfig	Automatically check for and update feature keys.
grep	Searches named input files for lines containing a match to the given pattern.
help	Returns a list of commands.
ifconfig or interfaceconfig	Configure and manage network interfaces including M1, P1, and P2. Displays currently configured interfaces, and provides an operations menu to create, edit, or delete interfaces.
last	Lists user-specific user information that includes ttys and hosts, in reverse time order or lists the users that are logged in at a specified date and time.
loadconfig	Load a system configuration file.
logconfig	Configure access to log files.
mailconfig	Mail the current configuration file to the address specified.

maxhttpheadersize	<p>Set the maximum HTTP header size for proxy requests; enter the value in bytes, or append a K to the number to indicate kilobytes.</p> <p>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 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.</p>
networktuning	<p>The WSA 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.</p> <p>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.</p> <p>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.</p> <p>The networktuning subcommands are:</p> <p><b>SENDSPACE</b> – TCP send-space buffer size; range is from 8192 to 131072 bytes; the default is 16000 bytes.</p> <p><b>RECVSPACE</b> – TCP receive-space buffer size; range is from 8192 to 131072 bytes; the default is 32768 bytes.</p> <p><b>SEND-AUTO</b> – 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 &gt; miscellaneous &gt; Would you like proxy to perform dynamic adjustment of TCP send window size? to disable send buffer auto-tuning.</p> <p><b>RECV-AUTO</b> – 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 &gt; miscellaneous &gt; Would you like proxy to perform dynamic adjustment of TCP receive window size? to disable receive buffer auto-tuning.</p> <p><b>MBUF CLUSTER COUNT</b> – 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: <math>98304 * (X/Y)</math> where X is gigabytes of RAM on the system and Y is 4 GB. For example, with 4 GB RAM, the recommended value is <math>98304 * (4/4) = 98304</math>. Linear scaling is recommended as RAM increases.</p> <p><b>SENDBUF-MAX</b> – Specify the maximum send buffer size; range is from 131072 bytes to 2097152 bytes; the default is 1 MB (1048576 bytes).</p> <p><b>RECVBUF-MAX</b> – Specify the maximum receive buffer size; range is from 131072 bytes to 2097152 bytes; the default is 1 MB (1048576 bytes).</p>

networktuning (cont.)	<p><b>CLEAN-FIB-1</b> – 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.</p> <p>Following any changes to these parameters, be sure to commit your changes and the restart the appliance.</p> <p><b>Caution</b></p>  <p>Use this command only if you understand the ramifications. We recommend using only with TAC guidance.</p>
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	<p>Enables or disables Path MTU Discovery.</p> <p>You might want to disable Path MTU Discovery if you need to packet fragmentation.</p>
ping	Sends an ICMP ECHO REQUEST to the specified host or gateway.
proxyconfig <enable   disable>	Enables or disables the Web Proxy.
proxystat	Display web proxy statistics.
quit, q, exit	Terminates an active process or session.
reboot	Flushes the file system cache to disk, halts all running processes, and restarts the system.
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.
rollovernow	Roll over a log file.
routeconfig	Configure destination IP addresses and gateways for traffic. Displays currently configured routes, and provides an operations menu to create, edit, or delete, or clear entries.
saveconfig	Saves a copy of the current configuration settings to a file. This file can be used to restore defaults, if necessary.
setgateway	Configure the default gateway for the machine.
sethostname	Set the hostname parameter.

<code>setntlmsecuritymode</code>	Changes the security setting for the NTLM authentication realm to either “ads” or “domain”. <ul style="list-style-type: none"> <li>• <code>domain</code> — 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.</li> <li>• <code>ads</code> — AsyncOS joins the domain as a native Active Directory member. Default is <code>ads</code>.</li> </ul>
<code>settime</code>	Set system time.
<code>settz</code>	Displays the current time zone and the time zone version. Provides an operations menu to set a local time zone.
<code>showconfig</code>	Display all configuration values. <b>Note</b> User passphrases are encrypted.
<code>shutdown</code>	Terminates connections and shuts down the system.
<code>smtpprelay</code>	Configure SMTP relay hosts for internally generated email. An SMTP relay host is required to receive system generated email and alerts.
<code>snmpconfig</code>	Configure the local host to listen for SNMP queries and allow SNMP requests.
<code>sshconfig</code>	Configure hostname and host key options for trusted servers.

sslconfig	<p>Commands for use of communications protocols TLS v1.x and SSL v3 with Appliance Management Web User Interface, Proxy Services (includes HTTPS Proxy and Credential Encryption for Secure Client), Secure LDAP Services (includes Authentication, External Authentication and Secure Mobility), as well as the Update Service.</p> <p><b>VERSIONS</b> – View and change the protocols enabled for specific services.</p> <p><b>COMPRESS</b> – Enable/disable TLS compression. Disabling is recommended for best security.</p> <p><b>CIPHERS</b> – Add/update cipher suites available to selected protocols.</p> <p>The default cipher for AsyncOS versions 9.0 and earlier is <code>DEFAULT:+kEDH</code>. For AsyncOS versions 9.1 and later, it the default cipher is  <code>ECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:    :!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES2    56-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA</code>. In both cases, this may change based on your ECDHE cipher selections.</p> <p><b>Note</b> However, regardless of version, the default cipher does not change when you upgrade to a newer AsyncOS version. For example, when you upgrade from an earlier version to AsyncOS 9.1, the default cipher is <code>DEFAULT:+kEDH</code>. In other words, following an upgrade, you must update the current cipher suite yourself; Cisco recommends updating to  <code>ECDH: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</code>.</p> <p><b>FALLBACK</b> – 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.</p> <p>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.</p> <p><b>Note</b> 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.</p> <p><b>ECDHE</b> – Enable/disable use of ECDHE ciphers for LDAP.</p> <p>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 <a href="#">SSL Configuration, page 12-22</a> for more information about specifying additional ciphers.</p> <p>If you experience these issues, use this option to disable or enable ECDHE cipher use for either or both features.</p>
status	Displays system status.

supportrequest	Send the support request email to Cisco IronPort Customer Support. This includes system information and a copy of the master configuration.
tail	Displays the end of a log file. Command accepts log file name or number as parameters.  example.com> tail system_logs example.com> tail 9
tcpservices	Displays information about open TCP/IP services.
techsupport	Provides a temporary connection to allow Cisco IronPort Customer Support to access the system and assist in troubleshooting.
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.  <b>Note</b> Cisco recommends you use level 0. Only use a different debug level when you need more detailed information to troubleshoot.
traceroute	Traces IP packets through gateways and along the path to a destination host.
tuiconfig tuistatus	These two commands are documented in <a href="#">Using the CLI to Configure Advanced Transparent User Identification Settings, page 5-9</a> .
updateconfig	Configure update and upgrade settings.
updatenow	Update all components.
userconfig	Configure system administrators.
version	Displays general system information, installed versions of system software, and rule definitions.
webcache	Examine or modify the contents of the proxy cache, or configure domains and URLs that the appliance never caches. Allows an administrator to remove a particular URL from the proxy cache or specify which domains or URLs to never store in the proxy cache.
who	Displays users logged into the system, for both CLI and Web interface sessions.  <b>Note</b> Individual users can have a maximum of 10 concurrent sessions.
whoami	Displays user information.



## Additional Resources

---

- [Cisco Notification Service](#), page C-1
- [Documentation Set](#), page C-2
- [Training](#), page C-2
- [Knowledge Base Articles \(TechNotes\)](#), page C-2
- [Cisco Support Community](#), page C-2
- [Customer Support](#), page C-2
- [Registering for a Cisco Account to Access Resources](#), page C-3
- [Third Party Contributors](#), page C-3
- [Cisco Welcomes Your Comments](#), page C-3

## 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](#), page C-3.

# Documentation Set

Related documentation for Cisco Web Security Appliances is available from the following locations:

Product	Link
Web Security appliances (Includes hardware documentation.)	<a href="http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html</a>
Content Security Management appliances (Includes hardware documentation.)	<a href="http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html</a>
Cisco Cloud Web Security (Includes hardware documentation.)	<a href="http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html</a>

# 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)

- 
- 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](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](#), page A-17.

## Registering for a Cisco Account to Access Resources

Access to many resources on Cisco.com requires a Cisco account.

If you do not have a Cisco.com User ID, you can register for one here:  
<https://tools.cisco.com/RPF/register/register.do>

## Third Party Contributors

Some software included within AsyncOS is distributed under the terms, notices, and conditions of software license agreements of FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc., and other third party contributors, and all such terms and conditions are incorporated in license agreements. The full text of these agreements can be found here:

[https://support.ironport.com/3rdparty/AsyncOS\\_User\\_Guide-1-1.html](https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html).

Portions of the software within AsyncOS is based upon the RRDtool with the express written consent of Tobi Oetiker.

Portions of this document are reproduced with permission of Dell Computer Corporation. Portions of this document are reproduced with permission of McAfee, Inc. Portions of this document are reproduced with permission of Sophos Plc.

## Cisco Welcomes Your Comments

The Cisco Technical Publications team is interested in improving the product documentation. Your comments and suggestions are always welcome. You can send comments to the following email address:  
[contentsecuritydocs@cisco.com](mailto: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.

■ Cisco Welcomes Your Comments



## End User License Agreement

---

- [Cisco Systems End User License Agreement, page D-1](#)
- [Supplemental End User License Agreement for Cisco Systems Content Security Software, page D-8](#)

## Cisco Systems End User License Agreement

**IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.**

CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT OR AVAILABLE AT THE TIME OF YOUR ORDER (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE REPRESENTING THAT YOU PURCHASED THE SOFTWARE FROM AN APPROVED SOURCE AND BINDING YOURSELF TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN APPROVED SOURCE, AND APPLIES ONLY IF YOU ARE THE ORIGINAL AND REGISTERED END USER PURCHASER. FOR THE PURPOSES OF THIS END USER LICENSE AGREEMENT, AN "APPROVED SOURCE" MEANS (A) CISCO; OR (B) A DISTRIBUTOR OR SYSTEMS INTEGRATOR AUTHORIZED BY CISCO TO DISTRIBUTE /

SELL CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS; OR (C) A RESELLER AUTHORIZED BY ANY SUCH DISTRIBUTOR OR SYSTEMS INTEGRATOR IN ACCORDANCE WITH THE TERMS OF THE DISTRIBUTOR'S AGREEMENT WITH CISCO TO DISTRIBUTE / SELL THE CISCO EQUIPMENT, SOFTWARE AND SERVICES WITHIN YOUR TERRITORY TO END USERS.

*THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER'S USE OF THE SOFTWARE (DEFINED BELOW), EXCEPT TO THE EXTENT: (A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND CISCO GOVERNING CUSTOMER'S USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE "CLICK-ACCEPT" LICENSE AGREEMENT OR THIRD PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION OR DOWNLOAD PROCESS GOVERNING CUSTOMER'S USE OF THE SOFTWARE. TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE (1) THE SIGNED CONTRACT, (2) THE CLICK-ACCEPT AGREEMENT OR THIRD PARTY LICENSE AGREEMENT, AND (3) THE AGREEMENT. FOR PURPOSES OF THE AGREEMENT, "SOFTWARE" SHALL MEAN COMPUTER PROGRAMS, INCLUDING FIRMWARE AND COMPUTER PROGRAMS EMBEDDED IN CISCO EQUIPMENT, AS PROVIDED TO CUSTOMER BY AN APPROVED SOURCE, AND ANY UPGRADES, UPDATES, BUG FIXES OR MODIFIED VERSIONS THERETO (COLLECTIVELY, "UPGRADES"), ANY OF THE SAME WHICH HAS BEEN RELICENSED UNDER THE CISCO SOFTWARE TRANSFER AND RE-LICENSING POLICY (AS MAY BE AMENDED BY CISCO FROM TIME TO TIME) OR BACKUP COPIES OF ANY OF THE FOREGOING.*

**License.** Conditioned upon compliance with the terms and conditions of the Agreement, Cisco grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees to an Approved Source. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by an Approved Source with the Software in any manner (including on CD-Rom, or on-line). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of the Software online at Cisco's website to obtain the necessary license key or license file.

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement or in the applicable purchase order which has been accepted by an Approved Source and for which Customer has paid to an Approved Source the required license fee (the "Purchase Order").

Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation permits installation on non-Cisco equipment) for communication with Cisco equipment owned or leased by Customer and used for Customer's internal business purposes. No other licenses are granted by implication, estoppel or otherwise.

For evaluation or beta copies for which Cisco does not charge a license fee, the above requirement to pay license fees does not apply.

**General Limitations.** This is a license, not a transfer of title, to the Software and Documentation, and Cisco retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Cisco or its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Except as otherwise expressly provided under the Agreement, Customer shall only use the Software in connection with the use of Cisco equipment purchased by the Customer from an Approved Source and Customer shall have no right, and Customer specifically agrees not to:

- (i) transfer, assign or sublicense its license rights to any other person or entity (other than in compliance with any Cisco relicensing/transfer policy then in force), or use the Software on Cisco equipment not purchased by the Customer from an Approved Source or on secondhand Cisco equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;
- (ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;
- (iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction or except to the extent that Cisco is legally required to permit such specific activity pursuant to any applicable open source license;
- (iv) publish any results of benchmark tests run on the Software;
- (v) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Cisco; or
- (vi) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Cisco. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by applicable law, and at Customer's written request, Cisco shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Cisco's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Cisco makes such information available.

***Software, Upgrades and Additional Copies.*** NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO MAKE OR USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF MAKING OR ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE TO AN APPROVED SOURCE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO CISCO EQUIPMENT SUPPLIED BY AN APPROVED SOURCE FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

***Proprietary Notices.*** Customer agrees to maintain and reproduce all copyright, proprietary, and other notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in the Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Cisco.

***Term and Termination.*** The Agreement and the license granted herein shall remain effective until terminated. Customer may terminate the Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under the Agreement will terminate immediately without notice from Cisco if Customer fails to comply with any provision of the Agreement. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer, all restrictions and limitations imposed on the Customer under the section titled "General Limitations" and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License Agreement" shall survive termination of the Agreement.

**Customer Records.** Customer grants to Cisco and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Cisco the appropriate license fees, plus the reasonable cost of conducting the audit.

**Export, Re-Export, Transfer and Use Controls.** The Software, Documentation and technology or direct products thereof (hereafter referred to as Software and Technology), supplied by Cisco under the Agreement are subject to export controls under the laws and regulations of the United States (U.S.) and any other applicable countries' laws and regulations. Customer shall comply with such laws and regulations governing export, re-export, transfer and use of Cisco Software and Technology and will obtain all required U.S. and local authorizations, permits, or licenses. Cisco and Customer each agree to provide the other information, support documents, and assistance as may reasonably be required by the other in connection with securing authorizations or licenses. Information regarding compliance with export, re-export, transfer and use may be located at the following URL:

[http://www.cisco.com/web/about/doing\\_business/legal/global\\_export\\_trade/general\\_export/contract\\_compliance.html](http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html).

**U.S. Government End User Purchasers.** The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which the Agreement may be incorporated, Customer may provide to Government end user or, if the Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in the Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

**Identified Components; Additional Terms.** The Software may contain or be delivered with one or more components, which may include third-party components, identified by Cisco in the Documentation, readme.txt file, third-party click-accept or elsewhere (e.g. on [www.cisco.com](http://www.cisco.com)) (the "Identified Component(s)") as being subject to different license agreement terms, disclaimers of warranties, limited warranties or other terms and conditions (collectively, "Additional Terms") than those set forth herein. You agree to the applicable Additional Terms for any such Identified Component(s)."

#### Limited Warranty

Subject to the limitations and conditions set forth herein, Cisco warrants that commencing from the date of shipment to Customer (but in case of resale by an Approved Source other than Cisco, commencing not more than ninety (90) days after original shipment by Cisco), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by Cisco is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided "AS IS". This limited warranty extends only to the Software purchased from an Approved Source by a Customer who is the first registered end user. Customer's sole and exclusive remedy and the entire liability of Cisco and its suppliers under this limited warranty will be (i) replacement of defective media and/or (ii) at Cisco's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to the Approved Source supplying the Software to Customer, within the warranty period. Cisco or the Approved Source supplying the Software to Customer may, at its option, require return of the Software and/or Documentation as a condition to the remedy. In no event does Cisco warrant that the Software is

error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Cisco does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

**Restrictions.** This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Cisco or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Cisco, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing or demonstration purposes. The Software warranty also does not apply to (e) any temporary Software modules; (f) any Software not posted on Cisco's Software Center; (g) any Software that Cisco expressly provides on an "AS IS" basis on Cisco's Software Center; (h) any Software for which an Approved Source does not receive a license fee; and (i) Software supplied by any third party which is not an Approved Source.

#### **DISCLAIMER OF WARRANTY**

**EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY CISCO, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT THAT ANY OF THE SAME CANNOT BE EXCLUDED, SUCH IMPLIED CONDITION, REPRESENTATION AND/OR WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD REFERRED TO IN THE "LIMITED WARRANTY" SECTION ABOVE. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY IN SUCH STATES. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.** This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

***Disclaimer of Liabilities - Limitation of Liability.*** IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, CANADA, JAPAN OR THE CARIBBEAN, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO ANY APPROVED SOURCE FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT).

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO CISCO FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID

FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT). NOTHING IN THE AGREEMENT SHALL LIMIT (I) THE LIABILITY OF CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS TO CUSTOMER FOR PERSONAL INJURY OR DEATH CAUSED BY THEIR NEGLIGENCE, (II) CISCO'S LIABILITY FOR FRAUDULENT MISREPRESENTATION, OR (III) ANY LIABILITY OF CISCO WHICH CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

***Disclaimer of Liabilities - Waiver of Consequential Damages and Other Losses.*** IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, THE CARIBBEAN OR CANADA, REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

IF YOU ACQUIRED THE SOFTWARE IN JAPAN, EXCEPT FOR LIABILITY ARISING OUT OF OR IN CONNECTION WITH DEATH OR PERSONAL INJURY, FRAUDULENT MISREPRESENTATION, AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF CISCO OR ANY APPROVED SOURCE OR THEIR SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, IN NO EVENT WILL CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, BE LIABLE FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, HOWSOEVER ARISING, INCLUDING, WITHOUT LIMITATION, IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF, IN EACH CASE, CISCO, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT FULLY APPLY TO YOU. THE FOREGOING EXCLUSION SHALL NOT APPLY TO ANY LIABILITY ARISING OUT OF OR IN CONNECTION WITH: (I) DEATH OR PERSONAL INJURY, (II) FRAUDULENT MISREPRESENTATION, OR (III) CISCO'S LIABILITY IN CONNECTION WITH ANY TERMS THAT CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

Customer acknowledges and agrees that Cisco has set its prices and entered into the Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

**Controlling Law, Jurisdiction.** If you acquired, by reference to the address on the purchase order accepted by the Approved Source, the Software in the United States, Latin America, or the Caribbean, the Agreement and warranties ("Warranties") are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Canada, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the Province of Ontario, Canada, notwithstanding any conflicts of law provisions; and the courts of the Province of Ontario shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Europe, the Middle East, Africa, Asia or Oceania (excluding Australia), unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of England, notwithstanding any conflicts of law provisions; and the English courts shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. In addition, if the Agreement is controlled by the laws of England, no person who is not a party to the Agreement shall be entitled to enforce or take the benefit of any of its terms under the Contracts (Rights of Third Parties) Act 1999. If you acquired the Software in Japan, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of Japan, notwithstanding any conflicts of law provisions; and the Tokyo District Court of Japan shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Australia, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of New South Wales, Australia, notwithstanding any conflicts of law provisions; and the State and federal courts of New South Wales shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in any other country, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.

For all countries referred to above, the parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement and Warranties shall remain in full force and effect. Except as expressly provided herein, the Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any Purchase Order or elsewhere, all of which terms are excluded. The Agreement has been written in the English language, and the parties agree that the English version will govern.

Product warranty terms and other information applicable to Cisco products are available at the following URL:

<http://www.cisco.com/go/warranty>

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

## IMPORTANT: READ CAREFULLY

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software product licensed under the End User License Agreement ("EULA") between You ("You" as used herein means You and the business entity you represent or "Company") and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.

In addition to the limitations set forth in the EULA on your access and use of the Software, you agree to comply at all times with the terms and conditions provided in this SEULA.

DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM CISCO OR AN AUTHORIZED CISCO RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

For purposes of this SEULA, the Product name and the Product description You have ordered is any of the following Cisco Systems Email Security Appliance ("ESA"), Cisco Systems Web Security Appliance ("WSA") and Cisco Systems Security Management Application ("SMA") (collectively, "Content Security") and their Virtual Appliance equivalent ("Software"):

- Cisco AsyncOS for Email
- Cisco AsyncOS for Web
- Cisco AsyncOS for Management
- Cisco Email Anti-Spam, Sophos Anti-Virus
- Cisco Email Outbreak Filters
- Cloudmark Anti-Spam
- Cisco Image Analyzer
- McAfee Anti-Virus
- Cisco Intelligent Multi-Scan
- Cisco RSA Data Loss Prevention
- Cisco Email Encryption
- Cisco Email Delivery Mode
- Cisco Web Usage Controls
- Cisco Web Reputation
- Sophos Anti-Malware
- Webroot Anti-Malware

McAfee Anti-Malware  
Cisco Email Reporting  
Cisco Email Message Tracking  
Cisco Email Centralized Quarantine  
Cisco Web Reporting  
Cisco Web Policy and Configuration Management  
Cisco Advanced Web Security Management with Splunk  
Email Encryption for Encryption Appliances  
Email Encryption for System Generated Bulk Email  
Email Encryption and Public Key Encryption for Encryption Appliances  
Large Attachment Handling for Encryption Appliances  
Secure Mailbox License for Encryption Appliances

### Definitions

For purposes of this SEULA, the following definitions apply:

"Company Service" means the Company's email, Internet, security management services provided to End Users for the purposes of conducting Company's internal business.

"End User" means: (1) for the WSA and SMA, the employee, contractor or other agent authorized by Company to access the Internet and the SMA via the Company Service; and (2) for the ESA, the email boxes of the employees, contractors, or other agent authorized by Company to access or use the email services via the Company Service.

"Ordering Document" means the purchase agreement, evaluation agreement, beta, pre-release agreement or similar agreement between the Company and Cisco or the Company and a Cisco reseller, or the valid terms of any purchase order accepted by Cisco in connection therewith, containing the purchase terms for the Software license granted by this Agreement.

"Personally Identifiable Information" means any information that can be used to identify an individual, including, but not limited to, an individual's name, user name, email address and any other personally identifiable information.

"Server" means a single physical computer or devices on a network that manages or provides network resources for multiple users.

"Services" means Cisco Software Subscription Services.

"Service Description" means the description of the Software Subscription Support Services at [http://www.cisco.com/web/about/doing\\_business/legal/service\\_descriptions/index.html](http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html)

"Telemetry Data" means samples of Company's email and web traffic, including data on email message and web request attributes and information on how different types of email messages and web requests were handled by Company's Cisco hardware products. Email message metadata and web requests included in Telemetry Data are anonymized and obfuscated to remove any Personally Identifiable Information.

"Term" means the length of the Software subscription You purchased, as indicated in your Ordering Document.

"Virtual Appliance" means the virtual version of Cisco's email security appliances, web security appliances, and security management appliances.

"Virtual Machine" means a software container that can run its own operating system and execute applications like a Server.

#### **Additional License Terms and Conditions**

##### LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

###### **License of Software.**

By using the Software and the Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, Cisco hereby grants to Company a nonexclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on Cisco's hardware products, or in the case of the Virtual Appliances, on a Virtual Machine, solely in connection with the provision of the Company Service to End Users. The number of End Users licensed for the use of the Software is limited to the number of End Users specified in the Ordering Documents. In the event that the number of End Users in connection with the provision of the Company Service exceeds the number of End Users specified in the Ordering Documents, Company shall contact an Approved Source to purchase additional licenses for the Software. The duration and scope of this license(s) is further defined in the Ordering Document. The Ordering Document supersedes the EULA with respect to the term of the Software license. Except for the license rights granted herein, no right, title or interest in any Software is granted to the Company by Cisco, Cisco's resellers or their respective licensors. Your entitlement to Upgrades to the Software is subject to the Service Description. This Agreement and the Services are co-terminus.

###### **Consent and License to Use Data.**

Subject to the Cisco Privacy Statement at <http://www.cisco.com/web/siteassets/legal/privacy.html>, Company hereby consents and grants to Cisco a license to collect and use Telemetry Data from the Company. Cisco does not collect or use Personally Identifiable Information in the Telemetry Data. Cisco may share aggregated and anonymous Telemetry Data with third parties to assist us in improving your user experience and the Software and other Cisco security products and services. Company may terminate Cisco's right to collect Telemetry Data at any time by disabling SenderBase Network Participation in the Software. Instructions to enable or disable SenderBase Network Participation are available in the Software configuration guide.

###### **Description of Other Rights and Obligations**

Please refer to the Cisco Systems, Inc. End User License Agreement, Privacy Statement and Service Description of Software Subscription Support Services.